DEPARTAMENTO DE ENGENHARIAS E CIÊNCIAS DA COMPUTAÇÃO

MESTRADO EM ENGENHARIA INFORMÁTICA E DE TELECOMUNICAÇÕES

UNIVERSIDADE AUTÓNOMA DE LISBOA

"LUÍS DE CAMÕES"

SISTEMA DE REGISTO DA PRODUÇÃO BASEADO EM BLOCKCHAIN

Dissertação para a obtenção do grau de Mestre em Engenharia Informática e de Telecomunicações

Autora: Maria Inês de Almeida Parreira

Orientador: Professor Doutor Mário Pedro Guerreiro Marques da Silva

Número da candidata: 30002953

Julho de 2023

Lisboa

Agradecimentos

Quero agradecer aos meus pais, por me apoiarem sempre e me possibilitarem uma educação no ensino superior.

Aos meus amigos, que sempre estiveram a meu lado nos bons e maus momentos e me deram força no desenvolvimento desta dissertação.

Também quero agradecer a todos os professores que me ensinaram bastante ao longo da Licenciatura e do Mestrado, para no futuro me tornar uma boa profissional.

E ao meu orientador que me ajudou e aconselhou no desenvolvimento desta dissertação, bastante importante na minha vida.

Resumo

O pressuposto desta dissertação é, primeiramente, levar o conhecimento ao limite sobre Blockchain, nomeadamente, as tecnologias que envolve, como funciona, vantagens e desvantagens na sua utilização, comparar à tradicional abordagem centralizada e dar a conhecer os métodos de validação mais importantes. Por outro lado, pretende-se levar o conhecimento ao limite sobre Cadeias de Abastecimento, como as etapas que envolve, vantagens, riscos que podem ocorrer e como evitá-los, como gerir uma cadeia sustentável, entender como se pode obter qualidade num produto e como é feito o seu rastreamento baseado em Blockchain.

Numa segunda fase, é apresentada uma forma de desenvolver um Sistema de Registo da Produção baseado em Blockchain, onde o utilizador é um fabricante. Este, deve autenticar-se, para poder registar os seus produtos. Posteriormente, cada produto é enviado para a rede Blockchain, de modo a ser validado por um nó validador aleatório, que é decidido pelo método de validação *Proof of Stake*, e, por fim, é adicionado à Blockchain.

Palavras-chave: Blockchain; Algoritmos de Consenso; Criptografia; Cadeia de Abastecimento.

Abstract

The purpose of this project is, firstly, to push the knowledge to the limit about Blockchain, namely, the technologies it involves, how it works, the advantages and disadvantages of using it, compare to the traditional centralized approach and make known the most important validation methods and, also, push the knowledge to the limit about Supply chains, like, the phases it involves, advantages, risks that may occur and how to avoid them, how to manage a sustainable supply chain, make known how to obtain product quality and how to manage its Blockchain-based traceability.

Secondly, it is shown a way to develop a Blockchain-based Production Registration System. Where the user is a manufacturer, who must authenticate himself, to register his products. Subsequently, each product is sent to the Blockchain network, in order to be validated by a random validator node, which is decided by the validation method Proof of Stake, and in order to be added to the Blockchain.

Keywords: *Blockchain; Consensus Algorithms; Cryptography; Supply chain.*

Índice

Lista de Fotografias/Ilustrações

Lista de Siglas e Acrónimos

P2P	Peer-to-Peer
SCM	Supply Chain Management
PoW	Proof of Work
BTC	Bitcoin
GPU	Graphics Processing Unit
ASIC	Application-Specific Integrated Circuit
DHT	Distributed Hash Table
IT	Information Technology
DLT	Distributed Ledger Technology
PoS	Proof of Stake
DPoS	Delegated Proof of Stake
PoA	Proof of Authority
PoC	Proof of Capacity
BFT	Byzantine Fault Tolerance
DBFT	Delegated Byzantine Fault Tolerance
ETH	Ethereum
TPS	Transações Por Segundo
SHA	Secure Hash Algorithm
NONCE	Number only used ONCE
IoT	Internet of Things
SCM	Supply-Chain Management
SSCM	Sustainable Supply-Chain Management
API	Application Programming Interface
AES	Advanced Encryption Standard
DES	Data Encryption Standard

1 Introdução

O conceito de Blockchain foi introduzido em 2008, quando alguém ou um grupo de pessoas conhecida(s) pelo pseudónimo Satoshi Nakamoto, decidiu criar uma Blockchain para transações de Bitcoin, que servisse como *Distributed Ledger*, isto é, um banco de dados distribuído entre múltiplos dispositivos conectados numa rede descentralizada que armazena registos de *timestamp* e assinatura digital, aos utilizadores [1]. Em português significa cadeia de blocos e garante segurança, imutabilidade, rastreabilidade e transparência distribuída por uma rede Peer-to-Peer (P2P) [2], [3].

Qualquer um pode confirmar transações sem necessitar de uma autoridade ou serviço central a autorizá-las, visto que, à medida que são feitas transações e, posteriormente, adicionadas ao *ledger* (livro-razão), como bloco de transações, estas são verificadas [4].

Esta tecnologia armazena informação que se encontra distribuída por diversos nós, que compõem uma rede, dificultando a alteração dos dados, porque cada bloco de transações depende do anterior e é necessário modificar os dados em todos os nós, para tornar a modificação credível [4].

Inspiradas pela Bitcoin, surgiram outras aplicações, como, por exemplo, Ethereum. No entanto, a Blockchain vai para além das criptomoedas. Nesse sentido, outros setores, com o intuito de serem mais transparentes, mais seguros e quererem poupar dinheiro e tempo, acederam a esta inovação, sendo alguns exemplos desses setores, serviços financeiros, serviços de votação, saúde, logística, etc. [5].

Para um sistema de registo de produtos, é necessário entender como são geridas as cadeias de abastecimento. Conhecida, em inglês, como *Supply Chain Management* (SCM), a gestão de cadeias de abastecimento consiste em gerir uma rede de produtos e serviços. Inclui, o movimento e armazenamento de matéria-prima, organização no inventário e produto final, desde o produtor ao consumidor [6].

Com o avanço constante e rápido das tecnologias, é importante ter em conta a segurança, tornar os sistemas mais autónomos e ser mais transparente, para que os consumidores tenham mais confiança nos produtos que usufruem. A Blockchain vem, possivelmente, ajudar nesse sentido, visto que poderá trazer mais segurança, autonomia e transparência, trazendo assim confiabilidade e, ainda, traz rastreabilidade em tempo real, como estipulado por W. Viriyasitavat, L. D. Xu, Z. Bi e A. Sapsomboon em [7], o que será necessário num sistema de registo de produtos.

1.1 Formulação do Problema

Para esta dissertação, o problema que surge é: Qual será o impacto da tecnologia Blockchain num sistema de registo de produtos?

Para resolver este problema, terá de ser feita uma análise da tecnologia Blockchain, saber como funciona, caraterísticas, vantagens e desvantagens, analisar porque seria uma melhor opção que a centralizada já existente no mercado. Por outras palavras, no âmbito desta dissertação deve ser feita uma pesquisa minuciosa desta tecnologia, de modo a obter um conhecimento aprofundado.

De seguida, proceder-se-á a um estudo da gestão de cadeias de abastecimento, mais especificamente, entender como funciona, no que consiste, suas caraterísticas e riscos. Serão mencionadas, de igual modo, algumas indústrias de cadeias de abastecimento e as suas necessidades nos tempos de hoje, etc.

Depois de se desenvolver essa pesquisa, será analisado o impacto desta tecnologia, quando associada a um sistema de registo de produtos e os benefícios que poderá trazer.

Nesta dissertação também constará uma parte prática, onde se irá criar um website para registo de produtos baseado em Blockchain, tornando possível uma análise tanto teórica como prática.

1.2 Objetivos

O objetivo geral desta dissertação é avaliar o impacto da tecnologia Blockchain num sistema de registo da produção.

É importante denotar que existem pesquisas sobre este tema, que ainda necessitam de aprimoramento, visto que a tecnologia Blockchain ainda está nas suas fases iniciais.

1.2.1 Objetivos Específicos

Para esta dissertação, pretendo:

- Analisar como se pode criar uma rede Blockchain e aplicá-la a um sistema de registo de produtos, tendo em conta a gestão de uma cadeia de abastecimento;
- Analisar se a escolha de uma abordagem descentralizada, sendo que a Blockchain se configura como melhor que uma abordagem centralizada, em funcionamento no mercado;
- Analisar o impacto que a tecnologia Blockchain terá num sistema de registo de produção, isto é, se é positivo ou negativo.

1.3 Justificação

Nos tempos de hoje, os consumidores exigem produtos com bons preços, serviços rápidos e, acima de tudo, que sejam seguros. Para isto acontecer, é necessário saber o histórico todo de cada produto, onde foram produzidos, como foram transportados, as condições a que estiveram sujeitos, se foram produzidos de forma sustentável, etc. Já existem serviços que façam essa rastreabilidade, mas são ou em papel ou em sistemas demasiado lentos, que não efetuam comunicações entre si, acabando por ser serviços centralizados, onde a informação se encontra armazenada num único nó, possuindo um único ponto de falha e possibilidade de manipulação. É necessário algo que seja realizado em tempo real, que seja imutável, que seja viável e que comunique entre si. Por isso, é necessária uma tecnologia como a Blockchain, que traz segurança, rastreabilidade em tempo real, comunica em Peer-to-Peer (P2P), é mais eficiente, é de menor custo e também traz transparência, que é crucial, entre outros aspetos [8].

Pretendo realizar esta investigação, visto que, com o avanço rápido da tecnologia, pretende-se melhorar a sua segurança e realizar atividades mais rapidamente e de forma autónoma, o que são alguns benefícios que a tecnologia Blockchain fornece.

Também intendo que esta dissertação sirva de apoio para avanços futuros desta tecnologia, de modo que diversos setores façam uso dela para fornecerem segurança, transparência e confiabilidade aos seus consumidores.

1.4 Estrutura

Este documento é composto por sete capítulos:

- Capítulo 1 – **Introdução**: Neste capítulo é demonstrada uma breve introdução do conceito de Blockchain, os objetivos desta dissertação, o problema e a justificativa para a escolha do tema.
- Capítulo 2 – **Tecnologia Blockchain**: Neste capítulo aprofundou-se a descrição do conceito de Blockchain, bem como as suas caraterísticas, vantagens e desvantagens do seu uso, etc. Também são descritos outros conceitos importantes para dar a conhecer melhor esta tecnologia e como funciona.
- Capítulo 3 – **Gestão de Cadeias de Abastecimento**: Neste capítulo introduziu-se e aprofundou-se a gestão de uma cadeia de abastecimento, etapas que a envolvem, vantagens, riscos, como garantir sustentabilidade, como rastrear um produto com base numa rede Blockchain, entre outros pontos importantes.

- Capítulo 4 – **Metodologia**: Onde é definido o método de pesquisa realizado para responder ao problema proposto.
- Capítulo 5 – **Sistema de Registo da Produção baseado em Blockchain**: Envolve a parte prática da dissertação, isto é, a criação de uma aplicação de um sistema de registo de produção baseado em Blockchain e a sua descrição, como foi desenvolvida e como pode ser usada.
- Capítulo 6 – **Conclusões**: Que conclusões foram tiradas na resolução deste trabalho.
- Capítulo 7 – **Sugestões para Trabalhos Futuros**: Melhorias que se pretende para trabalhos futuros, o que ainda não foi feito e o que poderá ser feito.

2 Rede *Blockchain*

Neste capítulo, irá ser feita uma descrição aprofundada sobre o que é a *Blockchain*, como funciona, as suas caraterísticas, vantagens e desvantagens, tipos de *Blockchain*, como é feita uma transação e mais. Também será mencionado o que é uma rede P2P, tipos de criptografia, assinatura digital mecanismos de consenso, mineração, entre outros temas, para levar o conhecimento ao limite desta tecnologia.

Antes de dar início ao capítulo, será feita uma breve introdução a alguns termos, como *Blockchain*, assinatura digital, *hash*, criptografia e algoritmos de consenso, que serão aprofundados mais adiante.

A *Blockchain* é uma rede que armazena os dados de forma distribuída e descentralizada, ou seja, sem intervenção de terceiros, transmitindo segurança. Apresenta um *ledger* onde qualquer transação efetuada, é armazenada e toda a rede toma conhecimento do ocorrido. Por isso, qualquer nó que seja adicionado à rede, recebe uma cópia desse *ledger* e, também, caso qualquer nó saia da rede, nenhuma informação é perdida [1].

Assim que as transações são guardadas, é criada uma assinatura digital ou "*hash*". É a partir dos *hashes* que os blocos se interligam. De tal modo, os *hashes* encontram-se criptografados, para manterem a segurança e integridade na rede. Por serem criptografados, também protegem os dados contra alguém com mau intento, que pretenda alterá-los, por exemplo, visto que, a alteração num bloco, resulta em todos os precedentes a ficarem alterados, facilitando a deteção, por parte dos nós, de tal erro [1],

Para uma transação ser adicionada à cadeia de blocos, é necessário ser validada, o que é conseguido por algoritmos de consenso, que traduzem confiança. Isto deve-se ao facto de todos os nós constituintes da rede, terem a função de acordar se uma devida transação pode ou não ser adicionada à rede. Só após validação é que o novo bloco é inserido na *Blockchain*, tornando-o público [1].

2.1 Centralizada vs Descentralizada

Para responder ao segundo objetivo específico, este capítulo compara uma abordagem centralizada a uma descentralizada, de modo a definir qual a melhor.

Numa empresa deve existir gestão de atividades de negócio numa estrutura organizacional. Têm a opção de escolher de entre duas estruturas organizacionais: centralizada e descentralizada [9].

Uma rede centralizada é constituída por um ponto central, que planeia, toma decisões e executa ações. Esse ponto central pode ser uma localização, administração/empresa ou um único indivíduo [9].

Esta abordagem era muito utilizada no passado, visto que se pretendia uma gestão realizada num único ponto. Também, demonstra facilidade de trabalho a ser efetuado pelos funcionários, liderança e coordenação de pessoal [9].

Uma empresa pode beneficiar com esta abordagem em termos de comunicação, visto que todos os funcionários sabem a quem devem reportar, em caso de dúvida, erros, etc. Facilita a distribuição de cargos e funções pelos funcionários, o que se traduz numa melhor organização. A tomada de decisões torna-se mais eficiente, por existir um grupo que toma as decisões e transmite aos níveis mais baixos da empresa, para implementarem essa decisões, reduzindo a ocorrência de replicação de tarefas. Como existe uma administração, existe supervisão, garantindo consistência e elevada qualidade de trabalho [9].

No entanto, os funcionários dos níveis mais baixos ao não tomarem decisões, podem ficar desmotivados caso não concordem com as decisões e, consequentemente, insatisfeitos. Por não existir descentralização, pode ocorrer sobrecarga de ideias que podem ser mal implementadas ou nunca chegarem a ser implementadas. E, também, pode originar atrasos, visto que é necessária comunicação entre executivos e funcionários e vice versa, sempre que decisões são tomadas e sempre que são implementadas [9].

Numa rede descentralizada, a gestão e tomadas de decisão são efetuadas por vários níveis da organização. Muitas empresas podem adotar esta abordagem como vantagem competitiva, visto que as pode destacar das restantes [9].

Esta abordagem possibilita tomada de decisões e resposta às mesmas de uma forma rápida. Aumenta a capacidade de expansão, por fornecer qualidade e transparência aos seus clientes. E, motiva os funcionários monetariamente, quando realizam tarefas extra, aprendem novas habilidades, tomam decisões ou supervisionam outros funcionários [9].

Por outro lado, como existe mínima ou nenhuma supervisão, não se verifica se todos estão a desempenhar as suas devidas funções. E, por existirem várias decisões a serem tomadas e implementadas, pode ocorrer conflito ou interrupções [9].

Nos seguintes pontos, são realçadas as diferenças entre ambas as abordagens [9]:

- A centralizada é gerida através de um ponto central, enquanto a gestão da descentralizada é distribuída por toda a rede;

- A centralizada é mais eficiente para uma empresa de menor dimensão e a descentralizada é mais indicada para uma de maior dimensão;
- A descentralizada demonstra mais eficiência e rapidez na tomada de decisões;
- A descentralizada não apresenta um único ponto de falha;
- O custo torna-se mais elevado numa rede centralizada, por necessitar de uma equipa grande. Na descentralizada, o custo é mais elevado na manutenção da rede.

Uns preferem uma abordagem centralizada, enquanto outros preferem uma descentralizada. Porém, de acordo com Ayushi Abrol [9], devido ao aumento de competitividade de negócio, muitas empresas optam pela descentralizada, com o intuito de tomarem decisões mais rápida e eficientemente.

De igual modo, várias empresas optam por ambas as estruturas, visto que não é possível obter centralização ou descentralização completas. Isto é, na centralizada implica que os superiores tomem todas as decisões e na descentralizada existe baixa ou nenhuma supervisão, o que não é o ideal, como já visto anteriormente. Por isso, é importante existir um equilíbrio [9].

2.2 Bitcoin

A *Bitcoin* é a primeira moeda digital descentralizada que usa tecnologia *Peer-to-Peer* (P2P), de modo a não necessitar de bancos ou de uma autoridade central para estabelecer transações, permite pagamentos em todo o mundo e possui baixas taxas de processamento [10].

2.2.1 Transações

Uma transação é quando um indivíduo envia a outro indivíduo um determinado valor, que possui. Este envio pode ser possível via, por exemplo, telemóvel.

Na *Bitcoin*, a transação é feita indicando o endereço para onde se pretende transferir, e a quantidade a transferir, sem necessitar de perceber o processo [11]. No entanto, para esta dissertação é importante entender como é que essa transação funciona, na prática.

Para assegurar a integridade das transações criadas na rede, é utilizada criptografia de chave pública. Sendo assim, cada participante possui pares de chaves públicas e de chaves privadas, tornando possível a transferência de *Bitcoin*. Onde uma chave pública é partilhada com todos os que desejam fazer uma transferência com um determinado indivíduo, e, uma chave privada é conhecida apenas pelo proprietário, autorizando o gasto de quaisquer fundos recebidos pela chave pública associada. Um utilizador, ao utilizar a sua chave privada, pode

assinar transações (assinatura digital), possuindo também o seu *timestamp*. Se esta transação for concluída com sucesso, é transmitida para a rede, sendo incluída na Blockchain [11].

Para realizar uma transação, são necessários três elementos [2]:

- **Chave privada**, do remetente da transação (armazenado na *wallet*)
- **Chave pública**, do destinatário da transação (similar ao iban do destinatário)
- **Montante** da transação.

Pode existir ainda [2]:

- **Endereço bitcoin**, que se encontra armazenado na *wallet* e que é usado em transações para verificar o valor da conta. Corresponde a uma versão reduzida da chave pública, porém não é possível gerar a partir desta.
- ***Seed phrase*** (frase de 12 palavras), que permite recuperar as chaves privadas e endereços de *wallet*. Permite, ainda, recuperar o acesso aos fundos, mesmo que se deixe de ter acesso à *wallet* original.

No caso de o utilizador perder a chave privada, a *seed phrase* e a password de acesso à *wallet*, perde as criptomoedas [2].

Para uma transação ser válida, é necessário que a quantidade de Bitcoin no input seja superior à que se pretende enviar e que o output tenha um valor associado.

2.2.2 Mineração

A mineração é a maneira como uma nova transação pode ser verificada/validada na rede, tornando-se também crucial na manutenção e desenvolvimento dos registos armazenados na Blockchain, por descobrir novos blocos e os interligar com blocos já existentes. [12]

Minerar *Bitcoins* implica um investimento imenso em hardware sofisticado, para um processamento matemático bastante complexo, denominado *Proof of Work* ou PoW, e em energia [2].

Devido à proteção do *Proof of Work* (definido em 2.8.1), a mineração é dificultada. No caso do *Bitcoin*, e por essa razão, o(s) primeiro(s) minerador(es) recebe(m) um determinado valor de *Bitcoin* após encontrarem a solução do problema matemático, sendo que esse valor de *Bitcoin* vai variando, que de acordo com [13]. De momento, o valor está nos 6.25 BTC, correspondendo a 128,623.87 €, em 27 de Outubro de 2022. Após a solução ser encontrada, a cada quatro anos ou a cada 210,000 blocos, a recompensa passa a metade [2].

2.2.2.1 *Como minerar Bitcoin?*

Para minerar *Bitcoin* é necessário, primeiro ter uma carteira, visto que é onde vai receber o pagamento da mineração. Esta carteira não será uma carteira normal. É uma conta online encriptada que permite o armazenamento e a transferência de *Bitcoin* [13]. De seguida, é necessário um software de mineração, que se pode adquirir gratuitamente, e conectá-lo ao hardware sofisticado, que requer um investimento imenso em, por exemplo, *Graphics Processing Units* (GPUs) ou *Application-Specific Integrated Circuits* (ASICs), que serão a opção mais provável, visto que estas máquinas constituem a maioria do hardware de mineração de Bitcoin [12].

As GPUs serviam o pressuposto de executar vários processos em paralelo, melhorando a eficiência na resolução de problemas. No entanto, as ASICs ultrapassaram as GPUs, por serem mais fortes, terem mais poder de *hashing* e mais eficiência de energia. Estes processamentos trazem despesas associadas, tanto na energia elétrica, como no custo de aquisição de equipamento [14].

2.3 *Peer-to-Peer* (P2P)

Uma rede *Peer-to-Peer*, ou rede ponto a ponto, é uma rede descentralizada que comunica de nó para nó, não necessitando de um servidor ou autoridade central. Permite cada nó funcionar tanto como cliente, como servidor, possibilitando partilha e armazenamento de ficheiros ou transações, sem auxílio de um intermediário [15]. Na Figura 1 é possível observar um exemplo de uma rede P2P.

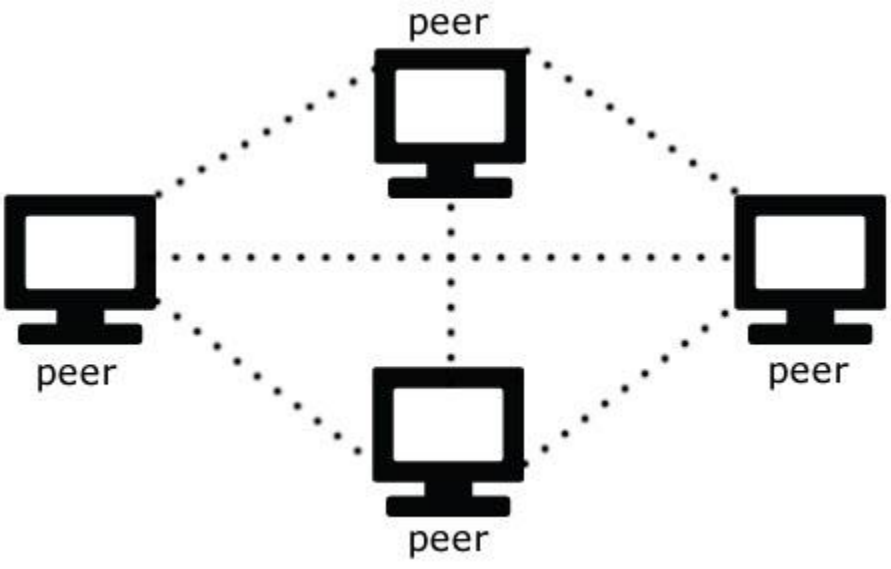

Figura 1- Exemplo de Rede P2P

Por ser descentralizada, cada nó pode armazenar a sua informação, transmitir ficheiros para outros nós e receber ficheiros provenientes de outros nós, o que não é possível numa rede centralizada. Esta descentralização, torna a rede mais rápida e eficiente. Este tipo de rede sobressai em relação à centralizada, por não apresentar um único ponto de falha, tornando-a bastante resistente a ciberataques [15].

As redes P2P podem ser categorizadas em quatro tipos principais, como:

- Redes P2P Puras – não são muito conhecidas, visto que não possuem nenhum sistema de gestão e o tamanho da rede é muito grande. Não dependem de nenhum servidor ou nó central para procurar ou partilhar dados [16].
- Redes P2P Não Estruturadas – fornece uma conexão simplificada com outros dispositivos. No entanto, por ser não estruturada, os utilizadores têm dificuldades em encontrar o conteúdo desejado, sendo que a pesquisa é enviada para toda a rede [17].
- Redes P2P Estruturadas – implementam uma *Distributed Hash Table* (DHT), permitindo a pesquisa de dados por funções *hash*. No entanto, por fornecerem eficiência, são dispendiosas na configuração e manutenção, e tendem a ser mais centralizadas [15].
- Redes P2P Híbridas – combina a rede ponto-a-ponto e a rede cliente/servidor (centralizada), sendo vantajoso para redes que necessitem de um servidor central com caraterísticas de P2P. Possui melhor desempenho do que as anteriores [15].

2.3.1 Vantagens e Desvantagens

As principais vantagens de uma rede Peer-to-Peer, são [18]:

- Por não necessitarem de um servidor central, tornam-se mais rentáveis.
- Não apresenta um único ponto de falha, por ser descentralizada.
- Se um par de nós sair da rede, não intervém no seu funcionamento, acontecendo o mesmo se entrarem mais nós, sendo que a rede gere facilmente o aumento da carga.

Apesar das vantagens, também possui desvantagens [18]:

- Apesar da segurança estar a melhorar, ainda traz alguns problemas desse tipo, por exemplo, se um nó for portador de um vírus, este se espalhará pelo resto da rede.
- Alguns utilizadores fazem uso de informação que não é sua e não acrescentam nada à rede, podendo vir a promover atividades ilegais ou antiéticas.
- Se a rede estiver offline, os dados não poderão ser copiados ou armazenados.

2.4 Blockchain

Como anteriormente referido, a Blockchain é uma rede descentralizada. Por essa razão, armazena a informação em diversos nós que compõem a rede, de forma distribuída. Usa as redes P2P de modo a fornecer um registo partilhado e confiável de transações, sendo as transações registadas com assinatura digital (ver 2.6) [15].

Cada bloco da Blockchain apresenta quatro campos [2]:

- **Previous *hash*** – *hash* do bloco anterior, que interliga os blocos, evitando fraude.
- **Data** – conjunto de transações do bloco. Após mineração e validação dos dados, estes são incluídos no bloco.
- ***Nonce*** – consiste num valor aleatório, que é utilizado para variar a saída do hash sum. Este elemento encontra-se presente apenas no algoritmo de consenso *Proof of Work* (2.8.1).
- ***Hash*** – é o valor *hash sum* obtido após passar "*previous hash*", "data" e "*nonce*" pelo algoritmo SHA-256, que corresponde à assinatura digital do bloco (como definido em 2.6).

Esta tecnologia permite a todos os utilizadores de uma rede validarem as suas transações, sem necessidade de uma autoridade central, traduzindo transparência e, consecutivamente, confiabilidade [15].

Toda a informação registada na Blockchain foi criptografada, com o intuito de garantir privacidade e segurança ao utilizador. Essa informação é armazenada e gerida de forma descentralizada, sendo que a maioria das decisões é baseada em consenso entre nós da rede [19].

2.4.1 Caraterísticas

A tecnologia Blockchain apresenta várias caraterísticas, que diferenciam em vários sites, artigos, etc. Após analisar esses sites, artigos, etc. foi decidido seguir as caraterísticas nomeadas em [20], por me parecer o mais adequado. Essas caraterísticas, são:

- **Imutabilidade** – torna a rede Blockchain permanente e sem a possibilidade de ser alterada, garantido o não repúdio dos dados. Isto funciona, porque cada nó possui uma cópia do *ledger* (livro-razão). Por isso, cada nó verifica e valida uma transação que se pretende adicionar à rede, com consentimento da maioria dos nós. Por outro lado, se a maioria não validar, será impossível adicionar o bloco de transação ao

ledger (livro-razão). Após a validação de uma transação, será impossível modificá-la.

- **Distribuída** – tal como anteriormente descrito, cada utilizador possui uma cópia do *ledger*, obtendo transparência. Esse *ledger* apresenta as informações sobre os restantes utilizadores da rede e as transações. O facto de ser distribuída, garante melhor desempenho. Por isso, o *Distributed Ledger Technology* (DLT) é bastante importante, sendo que:
    - Facilita a rastreabilidade;
    - Cada nó deve auxiliar na validação e manter o registo;
    - Qualquer alteração ao *ledger* e a sua validação será rápida, numa questão de segundos ou minutos, visto que não existe envolvimento de intermediários na rede;
    - Para adicionar um novo bloco, a maioria da rede deve verificar e validar a transação.
    - Todos os nós participantes são tão importantes como o seguinte, não havendo nenhum superior ou menos importante.
- **Descentralizada** – não existe uma autoridade central a tomar as decisões. Todos os nós participantes criam e mantêm a rede. Esta caraterística traz várias vantagens:
    - Torna a rede organizada e tolerante a falhas, o que significa que não existe um único ponto de falha.
    - Não existem riscos adicionais, visto que não há envolvimento de terceiros.
    - Facilita a transparência associada a qualquer utilizador, levando qualquer alteração na rede a ser mais concreta e facilmente rastreada, transmitindo, também, autenticidade**.**
    - Existe total controlo dos utilizadores sobre as suas propriedades.
- **Segurança** – conseguida devido às informações serem criptografadas com chaves assimétricas, e com assinatura digital, e por necessitar de todos os participantes da rede para verificarem e validarem uma transação. As informações são "criptografadas" com *hash*, atribuindo uma identidade única a cada parte dos dados que constituem a rede. Como cada bloco contém um *hash* único e o *hash* do bloco anterior, usado para interligar os blocos. Por isso, para alterar os dados de modo a ser credível, é necessário ir a todos os blocos (atual e todos os anteriores) e modificar

o ID de *hash* de cada um, o que é bastante improvável de acontecer, visto que é quase impossível um hacker conseguir fazê-lo.

- **Consenso** – ajuda a rede na toma de decisão rápida e imparcial, visto que a maioria dos nós ativos precisa de concordar com a decisão a ser tomada, rapidamente e para o bom desempenho do sistema. Não é necessário existir confiança entre nós, mas sim, existir confiança no algoritmo. Existem vários algoritmos de consenso (tal como descrito em 2.8), onde uma rede Blockchain deve apresentar um.
- **Liquidação mais rápida** – em comparação com um sistema bancário tradicional, uma rede Blockchain oferece liquidação de transferência de dinheiro mais rápida, isto é, não é propenso a lentidão do processamento de uma transação depois de finalizar a liquidação, o que acontece nos sistemas bancários tradicionais.

2.4.2 Benefícios

A *Blockchain* apresenta várias vantagens, que já foram mencionadas anteriormente e serão mencionadas ao longo desta dissertação. No entanto, aqui estarão nomeadas mais concretamente as principais, tanto como o seu papel numa rede Blockchain.

As principais vantagens da tecnologia *Blockchain* são [21]:

- **Segurança e Privacidade melhoradas** – por utilizar criptografia e assinatura digital, a *Blockchain* ajuda a evitar fraudes e ilegalidades. Permite anonimidade, o que também ajuda na privacidade, protegendo dados pessoais e requerendo permissões no acesso a certas informações. Por a informação ser armazenada de forma distribuída, dificulta o seu acesso por alguém com mau intento.
- **Maior transparência** – por utilizar um *Distributed ledger*, existe uma cópia dos registos ou transações por toda a rede. Por isso, qualquer utilizador que tenha autorização, pode aceder a essas informações em simultâneo, transmitindo transparência. Todas as transações seguem a imutabilidade propiciada por uma rede *Blockchain* (ler 2.4.1) e são, ainda, carimbadas com *timestamp* e assinatura digital (ler 2.6).
- **Rastreabilidade instantânea** – a *Blockchain* ajuda a rastrear produtos, com o intuito de verificar se são confiáveis, sustentáveis, legítimos, etc., podendo ser compartilhada informação sobre este produto, desde a origem até ao destino, o que é bastante importante numa cadeia de abastecimento e para indústrias onde os consumidores se preocupam com a qualidade do produto que pretendem adquirir.

- **Maior eficiência e velocidade** – transações podem ser realizadas mais rápida e eficientemente, por não existirem intermediários.
- **Automação** – pode-se automatizar uma transação com *Smart Contracts* (explicado em 2.9) que, por sua vez, também aumentam a eficiência e a rapidez do processamento. Esses *Smart Contracts* reduzem a intervenção humana e a dependência de terceiros na verificação do cumprimento de um contrato.

2.4.3 Desvantagens

Tal como qualquer tecnologia, a *Blockchain* também tem desvantagens, sendo estas [22]:

- **Elevado consumo de energia** – apesar de ser uma desvantagem, o consumo de energia é necessário para trazer vantagens, como manter um *ledger* em tempo real, transparência, rápidas validações de transações, ser tolerante a falhas, garantir que não existe inatividade e armazenar dados de forma imutável, resistente à censura e verificação de assinatura. No entanto, a verificação de assinatura pelo método do *Proof of Work* requer um elevado poder computacional para calcular operações matemáticas complexas, visto que cada transação necessita de ser assinada por um esquema criptográfico.
- Nem todos os nós podem fornecer a capacidade necessária, o que origina dois problemas:
    - ***Ledger* menor** – os nós não conseguem carregar a cópia completa da Blockchain, perdendo a imutabilidade e a transparência.
    - A Blockchain torna-se um **sistema mais centralizado**.

2.4.4 Tipos de *Blockchain*

Existem quatro tipos de *Blockchain* [23]:

- Pública
- Privada
- Híbrida
- Consórcio

Estes tipos serão analisados nos seguintes subcapítulos, demonstrando as vantagens e desvantagens de cada um e onde devem ser utilizados.

2.4.4.1 Blockchain Pública

Este tipo de *Blockchain* foi a base da Bitcoin na *Distributed Ledger Technology* (DLT). Apoiam a descentralização, removendo problemas originados da centralização, como baixa segurança e transparência [23].

Sendo pública, qualquer um pode ter acesso, apenas necessitando de Internet e um bom *hardware* para fazer parte da rede. Ainda, é possível verificar transações e registos, que ao serem validadas, deixam de poder ser alteradas [23].

Possui algumas vantagens, como [24]:

- O facto de ser **confiável**, visto que há algoritmos que detetam fraudes, os utilizadores não necessitam de se preocupar com o resto da rede.
- Ser **seguro**, não sendo necessário revelar a sua identidade para ser um nó válido na rede.
- **Transparência**, apresentando uma rede imensa que contém todos os registos verificados, sendo difícil perdê-los ou danificá-los.
- **Descentralização**, não por existir um nó central ou um super nó a manter a rede, mas sim por existir uma vasta rede de utilizadores a possuir uma cópia do *ledger* (livro-razão).

No entanto, também apresenta algumas desvantagens [24]:

- **Escalabilidade** – por ser uma rede de grandes dimensões, torna-se lenta, acabando por atrasar o processo de verificação de cada nó.
- **Consumo de energia** – por requerer um bom hardware, acaba por consumir muita energia.

Este tipo de Blockchain é mais indicado, por exemplo, para desenvolvimento de criptomoedas, que foi o caso, da Bitcoin e da Ethereum [24].

2.4.4.2 Blockchain Privada

A *Blockchain* privada é uma rede fechada, controlada apenas por uma entidade, sendo que só nós selecionados podem participar na rede, tornando-a mais centralizada [23].

Possui algumas vantagens [24]:

- **Rapidez** – por ser uma rede de menor dimensão, a taxa de transação torna-se mais elevada e os nós são verificados mais rapidamente.
- **Escalabilidade** – o tamanho da rede pode ser ajustado, manualmente.

- **Privacidade** – existe mais confidencialidade, isto é, não é permitida a observação de informação a utilizadores não autorizados.
- **Equilíbrio** – apenas alguns utilizadores têm acesso à transação, melhorando o desempenho da rede.

Mas demonstra, também, algumas desvantagens [24]:

- **Segurança** – as *Blockchains* deste tipo são mais vulneráveis, visto que, sendo o número de nós limitado, estão mais sujeitas a manipulação.
- **Confiabilidade** – por ser centralizada, os utilizadores acabam por não ter tanta confiança.
- **Contagem** – devido a ser uma rede de menor dimensão, se todos os nós ficarem offline, pode existir perda de registos/dados.

Uma Blockchain privada é recomendada para casos de cadeias de abastecimento e votação interna, por exemplo [23].

2.4.4.3 Blockchain Híbrida

Combina *Blockchain* privada (com permissão) com a pública (sem permissão), permitindo o controlo ao acesso de dados específicos, isto é, quem lhes pode aceder, permitindo ainda definir quais os dados que serão abertos ao público [23].

Numa *Blockchain* híbrida, os dados serem "abertos ao público", não significa, literalmente, que são tornados públicos, mas sim que podem ser verificados quando necessário, acedendo através de um *Smart Contract* (ler 2.9). Mesmo que seja um proprietário desta rede, não é possível alterar as transações [23].

A identidade de um utilizador é estritamente revelada quando existe uma transação entre esse utilizador e outro, sem esse acordo, a identidade do utilizador é mantida secreta de outros [23].

Algumas vantagens são conseguidas por uma *Blockchain* híbrida [24]:

- **Ecossistema** – não pode ser hackeado, visto que maior parte dos utilizadores não têm acesso à rede.
- **Custo** – só existe confirmação realizada por alguns nós, tornando-a barata.
- **Arquitetura** – é personalizável e mantém integridade, segurança e transparência.
- É possível escolher quais as transações que são tornadas públicas e quem participa nelas.

Existem, também, algumas desvantagens [24]:

- **Eficiência** – nem todos podem implementar este tipo de Blockchain.
- **Transparência** – algumas informações podem ser ocultas.
- E por último, apesar da vantagem do ecossistema, também apresenta desvantagem. Por ser um **ecossistema fechado**, inibe o interesse de utilizadores participarem ou contribuírem na rede.

Pode ser utilizada em, por exemplo, registos médicos, de modo a não existir transmissão de dados para terceiros. No entanto, um médico e o seu paciente podem aceder à informação a que lhes diz respeito, através de um *Smart Contract* (ler 2.9) [23].

2.4.4.4 Blockchain de Consórcio

É parecida com a *Blockchain* híbrida, visto que também possui caraterísticas de *Blockchains* privadas e públicas, mas é mais restrita, ou seja, limita o acesso a um grupo específico e não apresenta o risco de uma única entidade controlar a rede, sendo que mais que uma organização a pode gerir [23].

Os procedimentos de consenso são controlados por nós predefinidos, onde um nó validador pode iniciar, receber e validar qualquer transação, enquanto os nós não validadores, conhecidos como nós membros, apenas recebem ou iniciam transações [23].

A *Blockchain* de consórcio, também conhecida como Blockchain federada, apresenta as seguintes vantagens [24]:

- **Velocidade** – torna-se mais rápida por ter um número limitado de utilizadores, o que é útil para as organizações.
- **Autoridade** – as organizações podem descentralizar a rede, tornando-a mais segura.
- **Privacidade** – quem não tiver acesso à rede, não tem conhecimento da informação dos blocos verificados.

Por outro lado, também exibe algumas desvantagens [24]:

- **Aprovação** – como existem várias organizações envolvidas na rede, terão diferentes opiniões, tornando-a difícil de gerir.
- **Transparência** – informação pode ser escondida dos utilizadores, por parte das organizações.
- **Vulnerabilidade** – um nó membro pode ser comprometido, prejudicando o funcionamento da rede.

O uso de uma *Blockchain* de consórcio, de acordo com Christine Parizo [23], é ideal no rastreamento de alimentos, onde algumas organizações podem decidir quais os nós a validar as transações.

2.5 Criptografia

Algo muito importante para esta dissertação é entender como é que o uso da *Blockchain* pode ser segura. Para isso, neste capítulo serão mencionados dois conceitos, o de criptografia e o de *hashing* [25].

O uso de criptografia traz vários benefícios para uma rede de *Blockchain* [25]:

- **Criptografia** – utiliza criptografia assimétrica com o fim de garantir que uma transação proteja os dados e a comunicação contra divulgação e acesso não autorizados aos dados.
- **Imutabilidade** – muito importante para a *Blockchain*, vinculando os blocos com segurança por outros blocos e garantindo confiabilidade dos dados. Também garante confidencialidade, não sendo permitida a observação de informação a utilizadores não autorizados, integridade, a informação não pode ser maliciosamente ou acidentalmente alterada, sem o conhecimento de toda a rede, e privacidade.
- **Segurança** – por facilitar o registo de transações pela criptografia de dados e o acesso aos dados pelas chaves públicas e privadas. A manipulação de *hash* criptográfico com dados torna-se impossível, garantindo segurança na Blockchain.
- **Escalabilidade** – as transações são irreversíveis, garantindo confiabilidade na precisão do *Digital ledger* e permite armazenamento de infinitas transações, com segurança.
- **Não-repúdio** – fornecido pela assinatura digital, com o intuito de proteger contra qualquer negação de uma mensagem passada pelo seu originador. É resistente a colisões, isto é, não existe conflito entre mensagens enviadas e é fácil diferenciar uma da outra, visto que cada valor de entrada apresenta uma função *hash* exclusiva.
- **Impedir *hackers*** – também conseguida devido à assinatura digital, por evitar a modificação maliciosa dos dados, visto que se os dados forem alterados, a assinatura digital deixa de ser válida.

No entanto, também traz diversas limitações [25]:

- **Acesso difícil às informações** – quando as informações estão fortemente criptografadas e assinadas digitalmente, pode tornar o seu acesso complexo, mesmo que um utilizador seja autorizado.
- **Elevada disponibilidade** – garantir a disponibilidade de informação num determinado período de tempo, não é conseguida pela criptografia, o que é bastante importante para a segurança da informação.
- **Vulnerabilidade** – por requerer elevada complexidade e poder de computação, para resolver problemas matemáticos.
- **Custos elevados** – necessita de elevados investimentos de tempo e dinheiro. Sendo que precisa de configuração e manutenção de infraestrutura de chave pública, requerendo um grande investimento de dinheiro, e requer investimento de tempo, devido a técnicas criptográficas e processamento de informação.

A criptografia serve para proteger os dados contra acesso não autorizado, o que transmite confidencialidade. Na *Blockchain*, a criptografia protege as transações que ocorrem entre dois nós da rede. Pretende garantir segurança dos participantes, das transações, segurança contra *double-spending*[1] e, ainda, confidencialidade, ou seja, apenas um utilizador autorizado pode obter, ler e processar a transação [25].

A criptografia está relacionada com [25]:

- Encriptação – consiste em converter texto normal numa sequência de bits aleatória.
- Desencriptação – consiste em converter a sequência de bits aleatória em texto normal.
- Chave – auxilia na encriptação e desencriptação de uma mensagem.
- Cifra – algoritmo criptográfico que irá converter texto normal em texto cifrado.

Uma chave pode ser [26]:

- Pública – existem duas chaves, onde uma chave pública, utilizada pelo transmissor, serve para encriptar o texto normal em cifrado e uma chave privada, usada pelo recetor, para desencriptar o texto cifrado e torná-lo num texto normal, possibilitando a sua leitura. É assimétrica.
- Privada – uma mesma chave privada, que encripta e desencripta, sendo mais rápida que a chave pública. É simétrica, onde a chave é denominada chave secreta.

A criptografia pode ser dividida em dois tipos [2], [25]:

[1] *Double-spending*: quando um utilizador consegue gastar a mesma moeda digital duas ou mais vezes, para aproveitar os vários serviços, o que traduz numa falha técnica, permitindo a duplicação de dinheiro.

- Criptografia simétrica
- Criptografia assimétrica

2.5.1 Criptografia Simétrica

Na criptografia simétrica, demonstrada na Figura 2, é aplicado um algoritmo ao texto normal com o intuito de o cifrar. Para isso, o transmissor e o recetor necessitam de partilhar a chave secreta, de modo ao recetor poder desencriptar com essa chave a mensagem que o transmissor cifrou, também com essa chave [14].

Este tipo de criptografia, garante segurança de acordo com a dificuldade em adivinhar a chave utilizada para cifrar a mensagem. O tamanho de uma chave é diretamente proporcional à dificuldade que um indivíduo terá para aceder à mensagem cifrada, o que significa que quanto maior a chave, mais complicado será [14].

No entanto, também surge um problema, o facto de ser necessário partilhar a chave, torna-a vulnerável, sendo que um indivíduo com mau intento pode apoderar-se dela e, a partir daí, pode ler qualquer mensagem que seja trocada entre o transmissor e o recetor, pode falsificá-la e, ainda, trocar mensagens com ambos sem que nenhum se aperceba [14].

De entre vários algoritmos de cifragem, como AES, DES, etc., é possível destacar o DES (Data Encryption Standard), onde um utilizador vai usar a chave secreta para encriptar os dados, podendo, um recetor, posteriormente, desencriptar esses dados com a mesma chave secreta que lhe foi confiada [25].

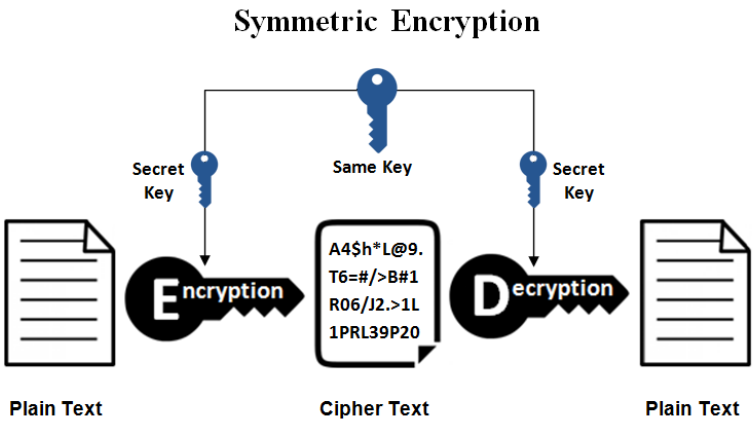

Figura 2 - Criptografia Simétrica [27]

2.5.2 Criptografia Assimétrica

A criptografia assimétrica pretende resolver o problema da vulnerabilidade associada à prévia distribuição das chaves da criptografia simétrica, garantindo que a partilha de chave será segura [14].

Neste tipo de criptografia, também conhecida como criptografia de chave pública, existem duas chaves, pública e privada, como se pode observar na Figura 3. A pública, é partilhada entre transmissor e recetor, possibilitando a troca de mensagens entre ambos. A privada, irá auxiliar na desencriptação da mensagem, ajudando também na verificação de assinatura digital (ver 2.6), o que é bastante importante na implementação de uma Blockchain [25].

A mensagem cifrada pela chave pública é apenas decifrada pela chave privada correspondente [14].

Esta criptografia pode trazer alguns problemas associados [14]:

- Processamento de elevada quantidade de dados torna-se lento, visto que os algoritmos de encriptação e desencriptação são muito complexos;
- Se alguém malicioso adquirir a chave privada, pode comprometer a segurança.

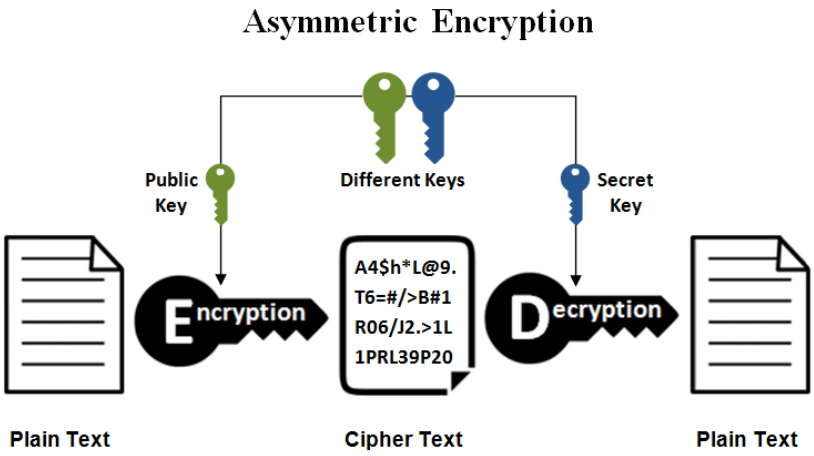

Figura 3 - Criptografia Assimétrica [27]

2.5.3 Hashing

Hashing acontece quando se transforma um input de tamanho variável num output de tamanho fixo, conhecido como digest, *hash* ou *hash* value. Para isso, é necessário utilizar funções *hash* implementadas por algoritmos de *hashing* [14].

O que torna as funções *hash* seguras e imutáveis, é o facto de qualquer modificação no input, por mais pequena que seja, apresentar resultados muito diferentes no output, facilitando

a verificação da integridade de um bloco, ao analisar a última *hash* criada. Também, é difícil voltar ao bloco original a partir da última *hash*, visto que o *hash* é aleatório e necessita de elevada potência computacional [14], [28].

Assim que uma transação é verificada, o *hash* é adicionado ao bloco, sendo também adicionado um *previous hash* ao bloco original (ler mais sobre *previous hash* em 2.7). Posteriormente, cada novo bloco terá a informação proveniente do bloco anterior, em forma de *hash*, e a nova *hash* com informação das novas transações. Deste modo, qualquer transação futura será baseada no bloco anterior [25], [28].

Uma função *hash* é uma "*one-way function*", isto é, é fácil obter um output a partir de um input, no entanto o contrário é difícil, por necessitar de elevado poder computacional [14].

Existem vários algoritmos de *hashing*, como MD-5, RIPEMD-160, SHA (1, 256, 384, etc.), Whirlpool, etc. [29]. No entanto, para esta dissertação será mencionado apenas o algoritmo SHA-256, por ser dos mais seguros, visto que é o mais complicado [30].

No topo da Figura 4, é possível observar uma frase que ainda não está codificada, isto é, ainda não está em *hash*. Porém, em baixo, a frase já se encontra em forma de *hash*.

Figura 4 - Exemplo de uma mensagem calculada por SHA-256 [31]

No entanto, ao modificarmos apenas o caracter "!" para ".", podemos observar pela Figura 5, que o *hash* está completamente diferente do original, sendo fácil para os nós da rede identificarem a alteração e não validarem a manipulação ocorrida, impossibilitando novas transações.

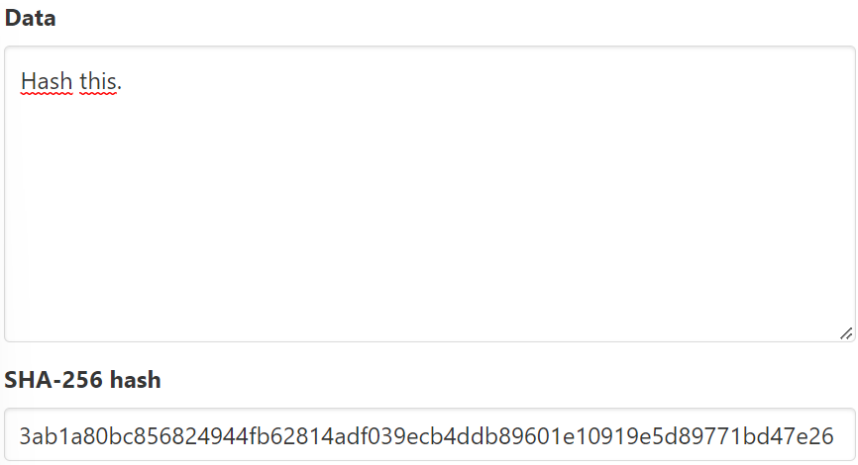

Figura 5 - Mensagem alterada calculada por SHA-256 [31]

O algoritmo SHA-256 gera um *hash* value quase único e de tamanho fixo de 256 bits. Permite verificar a integridade dos dados, desafiar a autenticação da *hash*, verificar imutabilidade, assinaturas digitais, entre outros. No entanto, devido aos avanços no hardware, também é possível desencriptar o *hash value* de SHA-256. Por isso, este algoritmo não é recomendado para proteger senhas de indivíduos maliciosos ou para outros casos de uso semelhantes [31].

Depois de analisar o que são algoritmos de *hash* e quais existem, surge também a questão "Para que servem?", existem várias respostas para tal [29]:

- **Armazenamento de senha** – é essencial guardar os registos das combinações utilizador/senha, que os utilizadores usam para aceder aos seus recursos. No entanto, um hacker pode conseguir entrar e facilmente roubar dados desprotegidos. Por isso, a *hash* vem garantir a segurança dos dados, sendo estes armazenados num estado codificado.
- **Assinaturas digitais** – uma pequena quantidade de dados prova a imutabilidade de uma nota desde o output até ao input.
- **Gestão de documento** – a autenticação de dados pode ser realizada por algoritmos de *hash*, onde a *hash* irá desempenhar uma função semelhante a um selo de aprovação. Um recetor pode gerar uma *hash* e compará-lo ao original. Se ambas as *hashes* forem iguais, os dados são autenticados e dados como genuínos. Se forem diferentes, determina-se que houve alteração no documento, resultando numa não autenticação dos dados.
- **Gestão de ficheiros** – empresas podem usar *hashes* para indexar dados, identificar ficheiros e excluir valores duplicados. O uso de *hashes* pode economizar o tempo, para um sistema com milhares de ficheiros.

2.6 Assinatura Digital

A assinatura digital é utilizada pela *Blockchain* com o intuito de verificar a integridade, autenticidade e não-repúdio da informação. Funcionam como uma assinatura em papel do mundo real. No entanto, é bastante mais segura e complicada, visto que é criada a partir de um processo matemático muito complexo, o *hashing*, e, também, por outros métodos criptográficos [2], [14], [32].

A criptografia assimétrica auxilia na verificação de assinatura digital, onde a chave pública encripta os dados e a chave privada, correspondente à chave pública respetiva, desencripta os dados [14].

Uma mensagem é transmitida ao recetor com a assinatura digital do transmissor associada. De seguida, o recetor verifica a viabilidade da assinatura, com a chave pública, que foi fornecida pelo remetente [14].

2.6.1 Como funciona a Assinatura Digital?

Neste subcapítulo, será analisado como funciona uma assinatura digital e como pode ser feita uma transação de um transmissor para um recetor, com o seu uso. Para tal, recorreu-se à Figura 6, que se analisou posteriormente. Também se recorreu ao algoritmo SHA-256 e à sua função hash, na explicação.

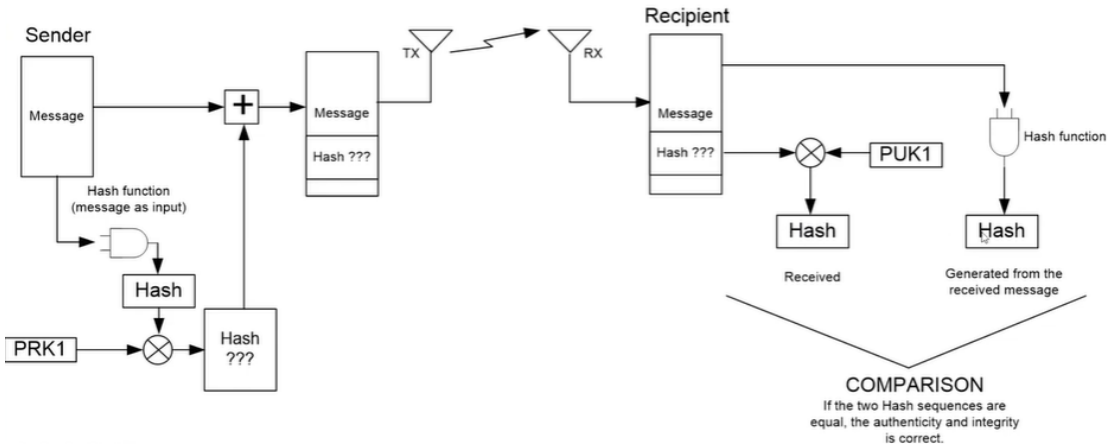

Figura 6 - Transação com Assinatura Digital [2]

Na Figura 6, é possível observar que um transmissor (*sender*) quer enviar uma mensagem. Para isso, é aplicada uma função *hash*, a essa mensagem, obtém-se um *hash* sum, constituído por 256 bits, originados pelo SHA-256, e cifra-se com a chave privada do transmissor (PRK1), obtendo a assinatura digital (*Hash* ???). Sendo transmitida a mensagem com a assinatura digital associada. Depois, o recetor "agarra" na mensagem e, a partir dela,

aplica a mesma função *hash*, obtendo os 256 bits. Como também recebeu a assinatura digital, vai decifrá-la com a chave pública (PUK1), que lhe foi fornecida pelo transmissor, obtendo, também, 256 bits. Se estes 256 bits forem iguais aos 256 bits gerados pela mensagem recebida, verifica-se que não existiu nenhum ataque e que se manteve integridade, autenticidade e não-repúdio. Se forem diferentes, então verifica-se uma manipulação dos dados e a transação será dada como inválida [2].

Devido à assinatura digital ser segura, tudo o que é armazenado numa rede Blockchain, é assinado digitalmente, o que é bastante vantajoso [2].

Tal como já foi estipulado, uma assinatura digital pretende fornecer autenticidade, integridade e não-repúdio dos dados. Onde a autenticidade garante que o autor da mensagem é o verdadeiro autor, isto é, o recetor reconhece-o pela chave pública do transmissor. A integridade garante que uma mensagem não é maliciosa ou acidentalmente alterada, quando transmitida, devido à função *hash*. Por fim, o não-repúdio, que garante que uma mensagem, após ser transmitida, não pode ser negada, excetuando quando, por algum motivo, existe comprometimento da chave privada [14].

No entanto, as assinaturas digitais também apresentam algumas limitações, como [14]:

- Algoritmo de *hash* – é necessário escolher um algoritmo com funções *hash* confiáveis e que tenha um bom sistema criptográfico, ou arrisca-se a corromper o sistema de assinaturas digitais.
- Chave privada – tem de ser mantida secreta ou também irá afetar o sistema, caso alguém malicioso se apodere dela, por exemplo.

2.7 Merkle Tree

Tal como o nome indica, é uma estrutura matemática de dados em forma de árvore. Efetua, de forma rápida, segura e eficaz, a verificação de consistência e conteúdo de grandes conjuntos de dados, mantendo a sua integridade, devido às funções *hash*. Pretende provar a veracidade de uma transação, isto é, se pertence ou não à rede. Para isso, apresenta uma *hash* de todas as transações que constituem o bloco [14].

É similar a uma árvore do mundo real, visto que apresenta folhas, mas também apresenta nós não-folha. No entanto, cada nó folha é um *hash* de dados transacionais e cada nó não-folha é um *hash* da *previous hash*, ou seja, é determinado pelo *hash* criptográfico dos nós filhos. Como é também conhecida como *Binary Hash Tree*, maior parte dos nós tem dois filhos, daí ser binária, porém também podem ter mais filhos [2], [33].

Esta árvore necessita que o número de transações seja par. Porém, se for ímpar, duplica-se o último *hash* de forma a existir um número de transações par [14].

Merkle Trees são originadas a partir do uso sucessivo do algoritmo SHA-256 até restar uma única *hash* a identificar a árvore completa, denominada *merkle root* ou *root hash*. São construídas de baixo para cima, por meio de transações individuais, conhecidas como IDs das transações [2].

O *merkle root* ou *root hash* está armazenado no cabeçalho do bloco e é um simples método matemático, com o intuito de confirmar os factos da *Merkle Tree*. Tem como principal objetivo garantir que os blocos são enviados ponto a ponto pela rede sem serem comprometidos, ou seja, sem danos ou alterações.

Uma *Merkle Tree* apresenta as seguintes vantagens [14]:

- **Integridade** – valida a integridade dos dados. Caso haja alteração numa transação ou na ordem das transações, irá alterar a árvore por completo, chegando, consequentemente, à *merkle root* e mudando o seu valor, o que invalida o bloco.
- Em comparação com outras estruturas de dados, **ocupa pouco espaço** no disco.
- **Eficiência** – a transferência dos dados é realizada de forma rápida, pela rede Blockchain.

Na Figura 7, está representada uma *merkle tree*. Pode-se observar que o bloco é constituído por cinco transações, "*Data1*", "*Data2*", "*Data3*", "*Data4*" e "*Data5*". Ao ser aplicada uma função *hash* a cada transação, são obtidas as seguintes *hashes*, "*Hash1*", "*Hash2*", "*Hash3*", "*Hash4*" e"*Hash5*", respetivamente, estando armazenados em nós folha. No entanto, devido ao número de transações ser ímpar, foi efetuada uma duplicação da última *hash*, para obter um número par. De seguida, realiza-se a *hash* dos pares de nós folha, isto é, combina-se a "*Hash1*" e a "*Hash2*", originando o nó pai "*Hash12*", a "*Hash3*" e "*Hash4*", que originam o "*Hash34*", e por fim, a "*Hash5*" com a "*Hash5*" duplicada, dando origem à "*Hash55*". Porém, como resultou no mesmo problema que anteriormente, é necessário duplicar a "Hash55", de forma a termos um número par. A seguir, é efetuada, novamente, a *hashing* dos pares de nós folha, obtendo-se a "*Hash1234*" e a "*Hash5555*". Finalmente, executa-se a *hashing* desse par, obtendo a *merkle root*, denominada "*Hash12345555*".

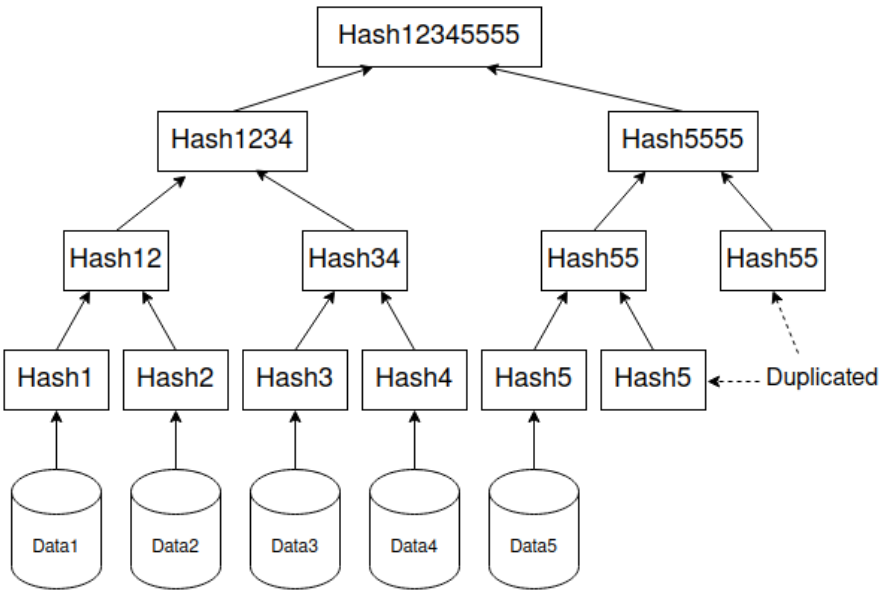

Figura 7 - Exemplo de uma Merkle Tree [34]

No entanto, uma *merkle tree* é muito mais complexa, visto que com o algoritmo SHA-256, cada ID de transação apresentará 256 bits, que representam 64 caracteres. Este é apenas um exemplo simples, para perceber melhor como funciona e porque é tão eficiente.

2.8 Algoritmos de Consenso

Para implementar uma rede Blockchain é necessário, para além dos tipos de Blockchain, também conhecer os algoritmos de consenso existentes.

Apesar de não existir uma autoridade central a validar e verificar transações, todas as transações são seguras e verificadas, o que é conseguido devido ao protocolo de consenso [35].

Um algoritmo de consenso tem como objetivo validar a autenticidade de uma transação e armazená-la no *ledger* distribuído, com o consentimento de todos os pares da rede, traduzindo confiabilidade [35].

Existem vários algoritmos de consenso, como PoW, PoS, DPoS, PoA, PoC, BFT, DBFT, entre outros [36]. No entanto, só alguns serão aprofundados nos seguintes subcapítulos, sendo estes: *Proof of Work* (PoW), *Proof of Stake* (PoS), *Delegated Proof of Stake* (DPoS) e *Proof of Authority* (PoA).

2.8.1 Proof of Work (PoW)

Este algoritmo de consenso é o mais antigo e foi usado, primeiramente, na Bitcoin [14].

Tal como o nome indica, existe um "trabalho", a ser realizado por mineradores, de modo a garantir integridade e verificar transações. Para isso, os mineradores vão resolver um puzzle,

calculando, sucessivamente, funções *hash*, através de tentativa e erro, ou seja, à força-bruta [2], [14].

O *Proof of Work* fornece proteção à rede, sendo que torna a validação, associada à mineração, difícil e aprova mais de metade dos utilizadores que a constituem, dificultando, de igual modo, a alteração de dados [2].

Na Figura 8, é possível observar o ciclo do *PoW*. Neste ciclo, os mineradores fazem variar o *Nonce*, calculam a função *hash* do bloco e vêm qual o valor obtido (*hash* sum). Se o valor for menor que um certo target predefinido, o *PoW* termina. Por outro lado, se não for menor, deve-se alterar o *Nonce*, novamente, várias vezes até determinar o valor *hash*. Isto transmite segurança à rede, pois torna muito difícil um hacker corrompê-la [2].

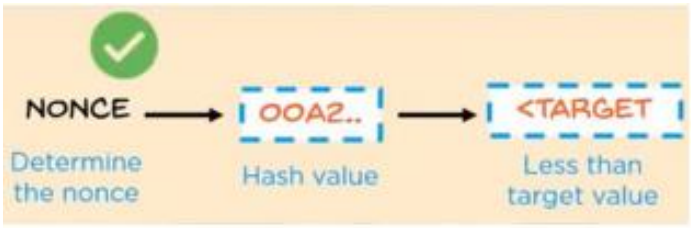

Figura 8 - Ciclo do PoW [2]

A *hash* target ou condição predefinida, que é calculada de acordo com a equação (2.1), determina a dificuldade da mineração, é expressa por um número de 64 dígitos e pretende manter a validação de um bloco num máximo de 10min. Por isso, os mineradores competem para encontrar a função *hash*, que é ajustada a cada 2016 blocos, que correspondem a aproximadamente 14 dias [2].

$$Hash\ Target_{(new)} = \frac{Hash\ Target_{(current)} * Avg.time\ taken\ to\ generate\ last\ 2016\ blocks_{(min.)}}{10_{min.}}$$

(2.1)

O grau de dificuldade da mineração depende do tempo que um bloco leva a ser minerado e é calculado pela equação (2.2). De acordo com a Figura 9, podemos observar que a dificuldade de mineração tem vindo a aumentar [2].

$$Difficulty_{(new)} = \frac{Hash\ Target_{(genesis\ block)}}{Hash\ Target_{(current\ block)}}$$

(2.2)

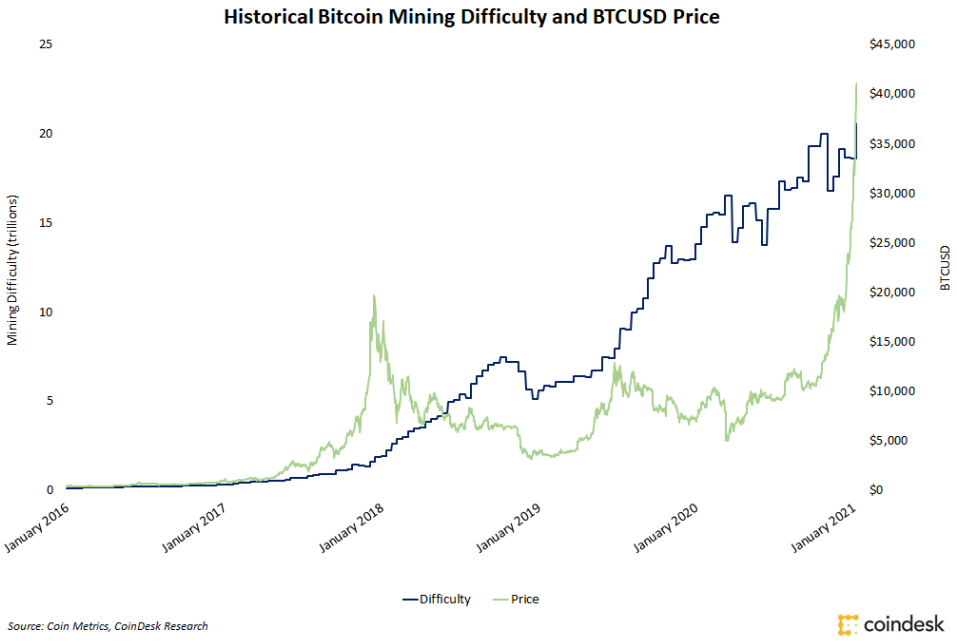

Figura 9 - Dificuldade de mineração de Bitcoin [37]

Como cada minerador está a tentar resolver o problema, isto é, das transações a serem validadas, e a colocar no seu devido bloco, podendo originar problemas de sincronização ou redundância com outros mineradores. Por isso, o PoW vai procurar um consenso, com todos os mineradores, para definir o bloco que será incluído na rede, sendo que os restantes serão eliminados, dando espaço para novas transações serem inseridas [14].

Para maior capacidade computacional, um minerador pode se juntar a um grupo, denominado *mining pool*, melhorando as hipóteses de ter sucesso na mineração e obter as recompensas de validação [14].

2.8.2 Proof of Stake (PoS)

O *Proof of Stake* veio substituir o *Proof of Work* em várias moedas como, por exemplo, a Ethereum, por tornar a validação mais eficiente e barata [2].

Fazer a transição do PoW para o PoS fornece não só o processamento de transações, já conseguido pelo PoW, mas também *smart contracts* de *stablecoins*, criação e venda de NFTs e mais, que, por exemplo, requer a *Ethereum*, e que o PoW não consegue oferecer. Por isso, o PoS vem ajudar nesse sentido, trazendo mais eficiência, redução de consumos energéticos e de taxas de interação com a rede *Blockchain* [14].

Não só fornece o que foi afirmado anteriormente, como, também, fornece a decisão de quais utilizadores da rede poderão criar os seus nós validadores e receber criptomoedas como recompensa. Para isso, os utilizadores necessitam de investir o seu próprio dinheiro, só assim

garantem que são fiáveis, tendo de depositar ou fazer um *stake* de uma dada moeda, que seja igual ou superior ao mínimo estipulado [14].

Os utilizadores também podem perder o seu investimento, devido ao *slashing*, isto é, se um nó ficar *offline* ou se for validado um bloco ilegal [14].

Para poder minerar/validar blocos, o sistema escolhe aleatoriamente um validador, ao contrário do PoW, onde os mineradores têm de competir. Além disso, um validador ainda tem que pagar um mínimo de 32ETH (corresponde a aproximadamente 39000€, em Novembro de 2022), e, ainda, necessitam de um elevado poder computacional, podendo se juntar a um grupo de investidores, denominado *staking pool*, podendo também receber as recompensas da validação, a única diferença era que, ao trabalhar em grupo, seria gerido por outro [14], [32].

2.8.3 Delegated Proof of Stake (DPoS)

Segue a mesma metodologia do *Proof of Stake*, com a diferença de os utilizadores poderem apostar tokens (criptomoedas) para votar em delegados ou testemunhas, isto é, utiliza um sistema de votação [38].

Tal como o PoS, o DPoS, possui utilizadores a investir uma quantia inicial de modo a poderem participar na rede, no entanto, no DPoS, os delegados ou testemunhas é que realizam essa tarefa, visto que foram eleitos para tal [32].

Os delegados serão também responsáveis por criar e verificar blocos, e, ainda, manter a segurança na rede. Podem existir entre 20 e 100 delegados para cada bloco a ser criado. Após um bloco ser criado e verificado, um delegado poderá receber a sua recompensa e partilhá-la com os seus eleitores [38].

Apesar de elegerem, os eleitores, também podem votar para eliminar os delegados, caso estes ajam maliciosamente na rede ou sejam ineficientes ou, até mesmo, não sejam honestos. Por isso, deve-se escolher um delegado de confiança, para proteger a rede e a comunidade [38].

2.8.4 Proof of Authority (PoA)

O *Proof of Authority*, que é utilizado, por exemplo, no Microsoft Azure, foi implementado com o intuito de melhorar a eficiência, de modo a serem realizadas mais transações por segundo (TPS) [39] As transações e os blocos só são validados por entidades validadoras, denominadas *supernodes*. Estes *supernodes* executam um software possibilitando a inserção das transações nos blocos [2].

Baseado em reputação, este algoritmo apresenta uma solução prática e eficiente nas redes Blockchain, em especial nas privadas. Por isso, um validador necessita de revelar a sua verdadeira identidade, colocando em risco a sua reputação, o que garante integridade e confiabilidade. Mas não é qualquer um que pode pertencer a esta rede, o processo de candidatura é extremamente difícil, de modo a reduzir os riscos de candidatar um validador malicioso, visto que o processo é difícil e duradouro, sem ser possível abandoná-lo rapidamente, pode desencorajar alguém com mau intento [14], [39].

O PoA traz algumas desvantagens, como o facto de não ser totalmente descentralizado, isto é, tem entidades a definirem quais candidatos serão validadores. Outra desvantagem é as identidades dos validadores serem públicas, possibilitando o roubo de identidade e manipulação, acabando por comprometer o sistema [14].

Este algoritmo de consenso é mais indicado para aplicações logísticas e para cadeias de abastecimento, por ser considerada uma solução eficaz e razoável [39].

2.9 Smart Contracts

Antes de definir *smart contracts*, deve ser definido um contrato, que é um acordo, vinculado por lei, entre duas partes, com o intuito de executarem tarefas ou transações individuais, como emprego, transações imobiliárias, etc. [40]

O conceito de *smart contract* foi introduzido por Nick Szabo, nos anos 90, que o definiu como sendo uma estrutura com o intuito de formalizar e proteger redes de computadores, combinando protocolos com interfaces do utilizador. Szabo pretendia que estes contratos servissem sistemas de crédito, processamento de pagamentos, gestão de direitos sobre conteúdos e outros serviços que envolvam contratos [41].

Estes contratos, pretendem corroborar a proteção de privacidade, permitindo, por exemplo, que dados protegidos pela privacidade sejam libertos de forma seletiva, apenas quando são requisitados especificamente [42].

Relativamente a uma rede *Blockchain*, são contratos digitais armazenados na *Blockchain* executados automaticamente, assim que condições predefinidas são atendidas. Automatizam a execução de um acordo, fornecendo aos utilizadores resultados em tempo real, sem a necessidade de um intermediário ou desperdiçar tempo. Podem, ainda, automatizar o fluxo de trabalho [43]. Facilitam a criação de protocolos *trustless*, isto é, dois utilizadores podem assumir compromissos e não necessitarem de confiar um no outro, visto que se as condições predefinidas não forem atendidas, o contrato será dado como inválido, não sendo

executado. Outra vantagem é o facto de não existirem intermediários, diminuindo os custos operacionais [41].

2.9.1 Como funcionam?

Funcionam como um contrato digital aplicado a um conjunto específico de condições predefinidas, sendo replicado e executado por todos os nós da rede. No estabelecimento das condições, as partes devem acordar em como as transações e os seus dados serão representados na rede, através de regras "se/quando… então…" que gerem essas transações, devem definir todas as limitações e definir uma estrutura para resolver contestações [41].

Um *smart contract* segue as seguintes etapas [44]:

- Existe um acordo entre duas partes, oficializando o contrato, que é um código de computador na rede *Blockchain*. O código, posteriormente, é armazenado num banco de dados distribuído, sendo impossível de o alterar, seguindo a imutabilidade requerida pela *Blockchain*.
- Assim que as condições predefinidas são atendidas, a transação será acionada, o que significa que alguém com mau intento não pode alterar ou falsificar o contrato.
- É efetuado o processamento da transação automaticamente, assegurando a segurança da transação.
- Assim que a transação for concluída, é adicionado um novo bloco e a *Blockchain* é atualizada, garantindo integridade, confidencialidade e autenticidade, visto que apenas as partes que participaram no *smart contract* é que podem aceder e/ou alterar os dados [41].

2.9.2 Vantagens

De seguida são apresentados os benefícios que um *smart contract* pode trazer a uma rede *Blockchain* [43]:

- **Velocidade, eficiência e precisão** – um *smart contract* é digital e executado automaticamente e em tempo real, assim que as condições predefinidas são atendidas, não existindo desperdício de tempo em emendar erros, que existem, por exemplo, em contratos físicos.
- **Confiança e transparência** – por não existir intermediários e o facto de os registos serem armazenados num *ledger* distribuído, torna-se desnecessário indagar a veracidade das transações e se foram modificadas.

- **Segurança** – sendo que a informação se encontra duplicada pela rede e interligada com os registos anteriores, os hackers terão mais dificuldades em comprometer a rede, visto que necessitariam de alterar a rede por completo para modificar um único registo.
- **Poupança** – o facto de não existirem intermediários, também reduz custos operacionais e atrasos.
- **Sustentabilidade** – visto que os *smart contracts* são digitais, não é necessário papel e não há poluição associada ao transporte de contratos físicos [45].

2.9.3 Casos de uso

Os *smart contracts* podem ser aplicados em várias áreas, em especial nas que requerem contratos tradicionais, como processos eleitorais, serviços de saúde, emprego, hipotecas, cadeias de abastecimento, etc. [45]. Dessas aplicações, é importante nomear as cadeias de abastecimento, que são relevantes para esta dissertação.

Associando *smart contracts* a dispositivos de *Internet of Things* (IoT)[2], pode facilitar a colheita e processamento de dados. Os dispositivos podem armazenar e processar os dados de forma segura e descentralizada, visto que a sua configuração é automatizada, garantindo a precisão e atualização dos dados e automatização da gestão [46]. Isto torna-se vital para uma cadeia de abastecimento, podendo registar todas as etapas de um produto, automaticamente e com segurança, melhorando a sua rastreabilidade e eliminando a ocorrência de erros, roubos e perdas de produtos ou informação [45].

[2] *Internet of Things* (IoT): rede de objetos físicos ("*things*"), veículos, eletrodomésticos, entre outros, que são incorporados com software, sensores e outras tecnologias que permitem a conexão e troca de dados entre dispositivos e sistemas, pela *Internet*.

3 Gestão de Cadeias de Abastecimento (SCM)

Neste capítulo, será dada a conhecer como é gerida uma cadeia de abastecimento, quais as etapas que envolve, vantagens, riscos que podem acontecer e como mitigá-los, como gerir uma cadeia sustentável, como obter qualidade num produto e como é feito o seu rastreamento baseado em Blockchain.

Na gestão de cadeias de abastecimento existe planeamento, implementação e controlo de aquisição, stock e armazenamento, transporte dos produtos (logística) e devolução, de forma eficiente. Gerir uma cadeia de abastecimento é muito importante e pode requerer maior investimento [47], [48].

Muitos usam erradamente a mesma definição para logística e cadeia de abastecimento. No entanto, a última é mais vasta e inclui logística no seu processo. Enquanto a logística abrange só a parte interna, uma cadeia de abastecimento vai para além disso, abrangendo também a parte externa, expandindo a coordenação dos fluxos de produtos e informações aos fornecedores e ao consumidor final [47].

A gestão de uma cadeia de abastecimento implica estratégia de negócios, software especializado e colaboração para funcionar. Quando se trata de uma empresa de grande dimensão, deve existir comunicação e trabalho em equipa entre fornecedores e fabricantes, para a cadeia se manter eficiente, poder gerir riscos e se adaptar rapidamente a mudanças [48].

Nos tempos de hoje, uma cadeia de abastecimento sustentável também é muito importante para as empresas, visto que os consumidores preocupam-se mais com esse aspeto, devido a quererem melhorar o meio ambiente e o bem-estar social [48].

Porém, o mais importante será criar confiança com os clientes, por isso é que para esta dissertação se pretende associar uma rede Blockchain à cadeia de abastecimento, visto que transmite transparência. Quando um consumidor compra um produto, espera qualidade e longevidade do mesmo. Mas, nem sempre é o caso, existem várias instâncias onde o consumidor compra algo que não tem a qualidade esperada, quebrando a sua confiança, tornando-se bastante difícil a uma empresa reaver esse cliente. Por isso, é estritamente necessário assegurar confiabilidade do produto, sem cometer fraude [49].

Segundo Nuno Almeida, *"We, as the consumer, value that we are buying good products"* [49], ou seja, atualmente os consumidores preferem comprar alimentos frescos, saudáveis e até pagariam extra para obter produtos e serviços mais sustentáveis. Também são mais cautelosos com o que compram e como gastam o seu dinheiro, indagando a veracidade e valor dos produtos que querem comprar, de modo a ficarem satisfeitos. São mais suscetíveis a

comprar algo de uma marca que seja transparente com os seus consumidores, o que resulta num ganho de confiança, por parte dos consumidores, pela marca.

Para existir confiança, uma empresa deve seguir os seguintes aspetos [49]:

- **Transparência** – visto que, mais do que nunca, os consumidores valorizam a transparência da empresa fornecedora. Uma das razões que leva os consumidores a não comprarem alimentos (fruta, vegetais, etc.) online, é o facto de não terem controlo sobre que produtos escolher, ou seja, não escolhem a qualidade.
- **Sustentabilidade** – mais consumidores preocupam-se com o meio ambiente, por isso exigem produtos sustentáveis, que não causem prejuízo ao ambiente.
- **Sociedade** – mais consumidores irão favorecer uma marca que desempenhe um papel no apoio à comunidade e que garante um impacto positivo na sociedade.

3.1 Etapas

Na gestão de uma cadeia de abastecimento, existem várias etapas que são requeridas, de modo a maximizar a eficiência e minimizar o custo da cadeia de abastecimento de uma organização. O consequente aumento de produtividade e eficiência traz bons resultados para uma empresa [50].

O papel de um gestor de uma cadeia de abastecimento, consiste nas seguintes etapas [50]:

- **Planeamento** – é a primeira etapa e visa atender às demandas do cliente e da manufatura. Uma empresa deve ter uma ideia da qual pretende que seja o produto final e o que necessita para chegar lá, como o fabrico, que envolve os materiais necessários para o seu desenvolvimento, capacidades e limitações do produto, que tipo de funcionários necessita para o seu desenvolvimento e, ainda, ter em conta o orçamento que têm.
- **Abastecimento** – esta etapa depende bastante da relação que uma empresa tem com os seus fornecedores, visto que estes são os que vão fornecer os materiais para o fabrico do produto e é pretendido que haja bom fluxo de trabalho, rápido e eficiente.
- **Manufatura** – nesta etapa ocorre o desenvolvimento do produto final, já com os materiais necessários e funcionários adquiridos para o fabricarem. É importante ter em conta os prazos e os recursos disponíveis. Para isso, esta fase está dividida em subtarefas, como montagem, teste, inspeção e empacotamento, de modo a gerir o

tempo. Quanto aos recursos, deve ser gerida a quantidade que foi adquirida e que está a ser utilizada, de modo a não esgotar e comprometer o fabrico.

- **Entrega** – depois de se ter o produto final, vem a parte da logística, isto é, a distribuição/transporte do produto para o consumidor final ou para uma loja ou supermercado, que o forneça ao consumidor final. Muitas empresas possuem recursos logísticos robustos, assegurando uma entrega pontual, segura e de baixo custo.
- **Devolução** – esta etapa, na maioria das vezes, pertence ao consumidor final, por ter adquirido um produto defeituoso ou por outro motivo, que o leva a querer devolver o produto. No entanto, uma empresa deve assegurar ao cliente os devidos recursos para receber produtos devolvidos e reembolsar os seus clientes, quer seja monetariamente, quer seja com um novo produto. Esta fase não envolve apenas o cliente e a empresa, pode envolver todos os que estavam envolvidos no processo de manufatura até à aquisição do cliente, com o intuito de não ocorrerem as mesmas falhas no sistema, no caso de ser uma devolução por defeito.

3.2 Vantagens

Na gestão de uma cadeia de abastecimento pode-se obter várias vantagens, que aumentam a margem de lucro, transmitem uma boa imagem para a empresa e originam uma maior vantagem em termos competitivos. Essas vantagens são [47], [48]:

- Torna mais fácil a previsão e atendimento às demandas do cliente;
- Maior eficiência de processo e menos suscetível a desperdiçar produtos;
- Melhor qualidade de produto, proveniente da estrutura das atividades ser bem organizada;
- A sustentabilidade, tanto ambiental como social, aumenta;
- Menor desperdício monetário;
- A parte da logística torna-se mais eficiente;
- Menor desperdício de tempo, originando mais lucros e satisfação do cliente;
- Aumento de confiabilidade, tanto dos fornecedores como dos clientes.

3.3 Riscos

Para uma cadeia de abastecimento, é importante que haja uma boa gestão, de forma aos produtos serem bem produzidos e em quantidade suficiente, para uma loja ou supermercado

não esgotar e para os clientes permanecerem satisfeitos. No entanto, podem ser muito suscetíveis a riscos, por exemplo, se uma entrega se atrasar, se um produto ultrapassar o orçamento estipulado, se tiver defeito, etc. Por isso, torna-se necessário gerir os riscos da cadeia, sendo que o gerente deve identificar todos os riscos possíveis de acontecer no seu negócio, saber delinear o que está ao seu alcance e o que não está, compreender o impacto e a probabilidade de um risco ocorrer e deve, acima de tudo, desenvolver um plano de gestão de riscos, para poder prevenir com antecedência o impacto [51].

Quando existe alguma falha nas etapas, nomeadas anteriormente, pode comprometer toda a cadeia, com atrasos, aumento de custos, pode diminuir a confiança dos consumidores, por motivos de atrasos, ou baixa qualidade de produto, ou por motivos éticos, etc. [51]

A seguir estão apresentados alguns tipos de riscos que podem acontecer, numa cadeia de abastecimento e como se pode diminuir ou atenuar o seu acontecimento [51]:

- Recursos Humanos, por exemplo, mudança de funcionários na empresa, por demissão, inatividade ou inexperiência:
  - Deve-se instruir a equipa devidamente, com as aptidões requeridas,
  - E recrutar funcionários competentes para o trabalho a desenvolver ou que aprendam rápido.
- Atrasos logísticos, por exemplo, na entrega internacional ou local:
  - Deve-se obter logística alternativa de outros países,
  - Aumentar a quantidade de pedidos e manter o stock local,
  - E verificar se o seguro cobre riscos que possam ocorrer.
- Fabrico, por exemplo, defeitos do produto:
  - Deve-se verificar a qualidade do produto,
  - E fazer a sua manutenção frequentemente.

3.4 SSCM – Sustainable Supply-Chain Management

A produção de elevadas quantidades de gases de efeito de estufa, é originada devido a várias empresas e às suas cadeias de abastecimento. Hoje, a logística é mais complexa, resultando em condições socioeconómicas de grande sucesso para as redes de cadeias de abastecimento. Por isso, várias empresas competem pelas inovações orientadas à sustentabilidade [52].

Uma cadeia de abastecimento sustentável (SSCM), segue as etapas de uma SCM, mencionadas anteriormente, fazendo gestão de materiais, informações e orçamento, e, ainda,

origina colaboração entre empresas, levando em conta opiniões de clientes e demandas das partes interessadas sobre aspetos económicos, ambientais e sociais, para melhorar a sustentabilidade. Os objetivos da SSCM são fornecer lucro a curto e longo prazo, competitividade entre empresas e sua resistência. Sendo assim, a SSCM tem o intuito de manter a estabilidade ambiental, económica e social, para melhorar a sustentabilidade a longo prazo numa SCM [52].

De acordo com R. Dubey, A. Gunasekaran, T. Papadopoulos, S. Childe, K. Shibin e S. Wamba [52], existem vários pontos muito importantes a analisar e que uma empresa deve seguir, para melhorar a sua sustentabilidade e transmiti-la aos seus consumidores. Desses pontos foram realçados:

- **Armazém verde** – grande parte dos produtos fabricados utilizam embalagens não sustentáveis. No entanto, hoje, muitas empresas usam embalagens reutilizáveis, o que originou redução de custos e de desperdícios. Para melhorar a sustentabilidade num armazém, é importante maximizar a utilização da área de armazenamento, minimizar o custo de armazenamento e de recuperação e minimizar o uso de energia.
- **Colaboração estratégica do fornecedor** – colaboração no planeamento, previsão e sistemas de reabastecimento, melhora o aspeto financeiro de uma empresa, conseguindo iniciativas de sustentabilidade na cadeia.
- **Conservação do ambiente** – se uma empresa se preocupar com este aspeto verá impactos diretos na sua cadeia e na vantagem competitiva. Isto é conseguido se uma organização melhorar a precisão da previsão de demandas e a eficiência energética, investir numa tecnologia de redução de carbono, etc.
- **Otimização na logística** – pode ser melhorando a velocidade, rota, carga e natureza do transporte, utilizando combustíveis alternativos ao invés de combustíveis fósseis, etc., o que melhora a margem de lucro e o controlo de emissão de gases de efeito de estufa.
- **Valores sociais e ética** – uma empresa deve ter uma ética forte para conseguir melhor sustentabilidade. Este aspeto origina colaborações entre empresas, abastecimento ético e mais compras efetuadas pelo consumidor final.

3.5 Garantir valor de produto na Blockchain

Nos tempos de hoje, os consumidores estão mais informados, por isso, fazem mais exigências e, também, devido ao avanço rápido da tecnologia, muitas indústrias partilham

algumas necessidades. De seguida são apresentados alguns desses setores com as necessidades requeridas [49]:

- Cadeia de alimentos e bebidas:
    - Transparência e qualidade dos produtos,
    - Unidades digitais que sejam impossíveis de copiar, de modo a não existir risco de "dupla venda" ou produtos de qualidade inferior,
    - Não seja necessário divulgar os dados de produção a uma parte central ou a intermediários,
    - E maior investimento em IT e interoperabilidade entre diferentes sistemas.
- Retalho:
    - Anti falsificação,
    - Sustentabilidade da produção,
    - Transparência e qualidade dos produtos,
    - Não seja necessário divulgar os dados de produção a uma parte central ou a intermediários,
    - E criação de programas de fidelidade.
- Logística:
    - Rastreamento em tempo real,
    - Gestão automatizada de stock,
    - Atualizações em tempo real,
    - E processos comerciais e de aquisição automatizados e interoperáveis.

Uma das questões levantadas para esta dissertação é: Será que a Blockchain pode ajudar na garantia de valor? De acordo com Nuno Almeida [49], a Blockchain pode ajudar, visto que:

- Fornece confiança e transparência ao consumidor final, compartilhando dados registados na Blockchain desde a produção até à distribuição e disponibilizando certificações e validações de terceiros confiáveis;
- Cria uma relação de confiança com os parceiros do ecossistema com base na transparência e automatiza processos administrativos, contratos e pagamentos para focar nas operações;
- Padroniza os formatos de dados para melhor interoperabilidade e aprimoramento da integridade e qualidade dos dados para apoiar a tomada de decisões;
- Combate a falsificação e fraude e monitoriza os canais de distribuição graças à rastreabilidade de todas as ações realizadas e ao seu registo num *ledger*;

- Possui melhor relação com o consumidor final e permite uma maior personalização devido à criação de uma ligação única com o produto, que é acompanhada ao longo do seu ciclo de vida, incluindo nos mercados secundários.

3.6 Rastreamento fornecido pela *Blockchain*

O rastreamento pode ser definido como a capacidade de *track* e *trace* de informação. Onde o *tracking* consiste no rastreamento de um produto desde a origem até ao consumidor final. E o *tracing* é o contrário, isto é, o rastreamento do consumidor final até à origem [53].

O uso de rastreamento numa cadeia de abastecimento pode originar transparência para a mesma. No entanto, as soluções de rastreamento já exigentes são centralizadas, o que não é preferível para as cadeias de abastecimento, que ficam sujeitas a vários problemas, como manipulação de dados, ponto único de falha, etc. Por isso, para mitigar esses problemas, originados em sistemas centralizados, utilizam-se soluções de rastreamento baseadas em Blockchain, que por ser descentralizada, não terá um único ponto de falha; dificilmente se conseguirá manipular os dados, visto que a rede toda possui uma cópia do *ledger*, podendo verificar e validar cada transação, o que garante transparência, etc. [53].

O uso de Blockchain numa cadeia de abastecimento, pode atenuar riscos, como quebra de infraestrutura de informação, atrasos de informação, falta de transparência na informação, falta de compatibilidade em IT entre parceiros da cadeia e segurança de Internet reduzida. E ao integrar tecnologias como *Smart Contract* e *Internet of Things* (IoT), possibilita um melhor rastreamento baseado em *Blockchain* [53]. Por exemplo, quando um *smart contract* é configurado para rastrear um produto desde o seu fabrico até ao consumidor final. Sendo que, o *smart contract* pode automatizar o pagamento assim que o produto é entregue, possibilitando, ainda, ao consumidor, visualizar o seu produto à medida que passa por cada etapa da SCM [46].

O valor da Blockchain em sistemas de rastreamento é fornecido por informações em tempo real, transparência e confiabilidade nos dados. Permite agilizar os processos internos e comunicar valor aos clientes e, ainda, pode fazer uma empresa destacar-se à medida que os consumidores fazem novas exigências, o que é bastante benéfico para qualquer cadeia de abastecimento [49].

4 Metodologia

Para atender aos objetivos específicos requeridos para esta dissertação, a pesquisa foi dividida em duas partes: pesquisa teórica e pesquisa prática, como demonstra o diagrama da Figura 10. Na teórica, realizaram-se pesquisas exaustivas de revisão de literatura, em *websites* e artigos da IEEE Xplore, Google Scholar, Science Direct, entre outros, de modo a ir ao limite do conhecimento sobre Blockchain, Cadeias de abastecimento e como se podem envolver, para, posteriormente, se criar um sistema de registo de produção baseado em Blockchain.

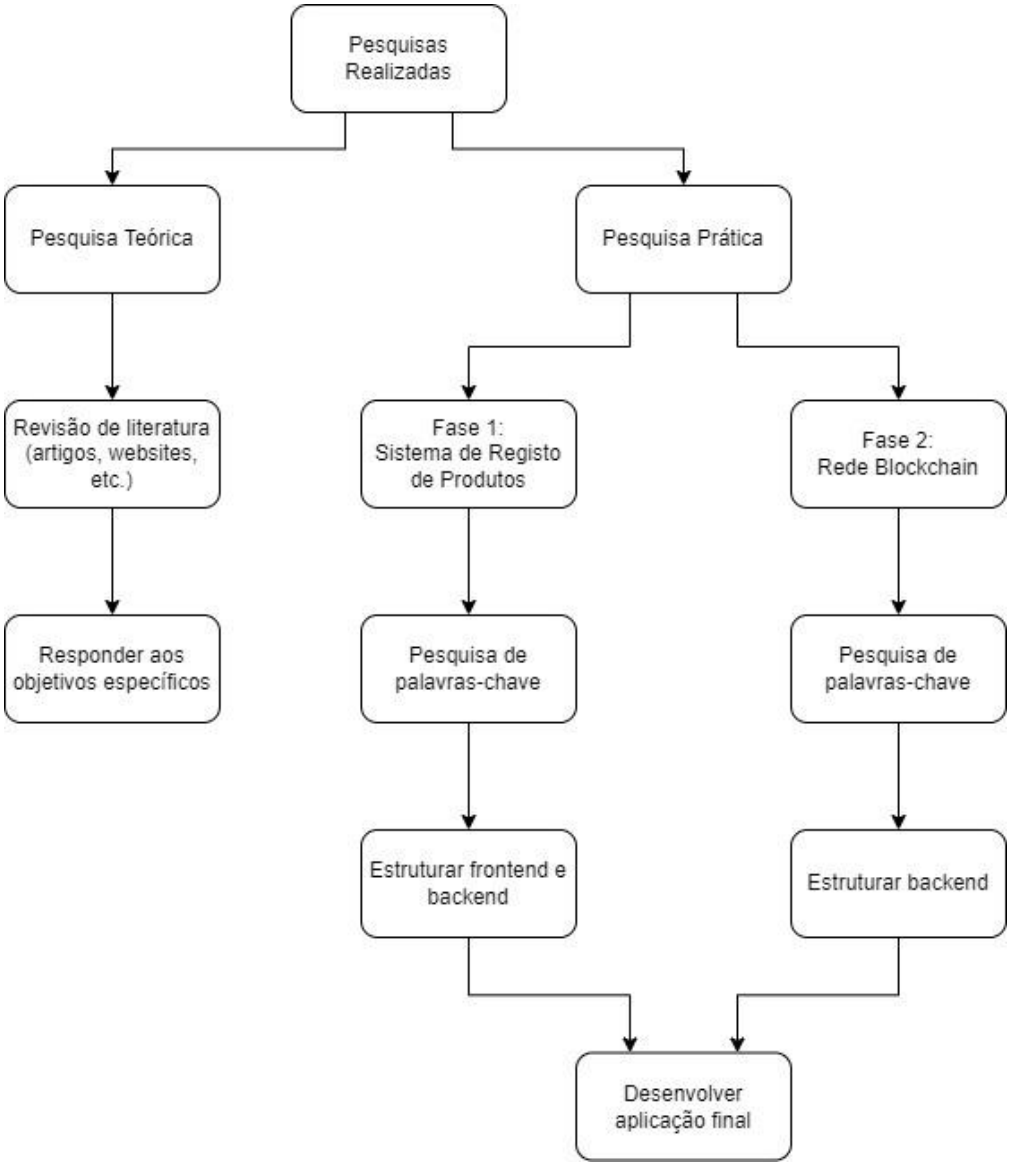

Figura 10 - Diagrama de Pesquisas Realizadas

Com o intuito de associar a rede Blockchain, na sua forma mais recente, a uma cadeia de abastecimento, foram selecionados vários artigos e *websites*, entre 2018 e 2022, com informação sobre os temas principais e as suas envolventes, para obter um conhecimento aprofundado.

Para cada artigo, foram examinados o título e o *abstract*, de modo a analisar se estes artigos se aplicavam ao caso de estudo e para obter melhor qualidade de pesquisa, eliminando os artigos que não se focavam, tanto, nos aspetos principais requeridos para esta dissertação. Enquanto para os *websites*, foram analisados os títulos e/ou subtítulos.

Para responder a cada objetivo específico, teve-se em conta os seguintes aspetos:

- **Objetivo específico 1**: Analisar como se pode criar uma rede Blockchain e aplicá-la a um sistema de registo de produtos, tendo em conta a gestão de uma cadeia de abastecimento.
    - Para atender a este objetivo, foi necessário não só entender como é constituída uma rede Blockchain, como funciona, caraterísticas, as tecnologias que a envolvem e como funcionam na rede. Mas, também, compreender uma cadeia de abastecimento, como é gerida, como funciona, como é feito o rastreamento, como se pode obter sustentabilidade nos produtos, etc.
- **Objetivo específico 2**: Analisar se a escolha de uma abordagem descentralizada, sendo esta a Blockchain, é melhor que uma abordagem centralizada, que já existe no mercado.
    - Aqui foi necessário comparar as duas abordagens, analisando as suas vantagens e desvantagens e as suas diferenças.
- **Objetivo específico 3**: Analisar o impacto que a tecnologia Blockchain terá num sistema de registo de produção, isto é, se é positivo ou negativo.
    - Para analisar o impacto de uma rede Blockchain num sistema de registo de produção, é necessário associar os dois, tanto numa fase teórica, que já foi realizada, como numa fase prática, que será analisada no próximo capítulo, com o pressuposto de chegar a uma conclusão se o impacto será positivo ou negativo.

Para a pesquisa prática, foi necessário pesquisar várias combinações de palavras-chave, no Youtube. Após essas pesquisas, foi decidido que o sistema seria desenvolvido no VS Code, pois facilitava a criação de um website com a integração de bases de dados e da rede blockchain. Relativamente à linguagem de programação escolhida para o desenvolvimento da rede Blockchain, optou-se pelo JavaScript. Com estas decisões, a forma de pesquisa de palavras-chave, tornou-se mais concreta, facilitando o método de pesquisa. Essa pesquisa foi dividida

em duas fases: sistema de registo de produtos e rede Blockchain, como se pode observar no diagrama da Figura 10.

Na primeira fase, foram pesquisadas palavras-chave, como "*product register system in javascript*", "*blockchain supply chain project" "sign up form" "login form" "product registration form"*, etc. Numa segunda fase, as palavras-chave foram, por exemplo, "*blockchain supply chain app*", "*blockchain in javascript*", etcForam feitas estas pesquisas com o intuito de decidir como construir a aplicação, tanto em *frontend,* como em *backend*.

Com a fase 1, ficou-se com uma ideia de como seria construída a parte de *frontend*. No entanto, para a fase 2, foi mais complicado, visto que não existia muita informação onde basear, dificultando a associação de ambas as fases.

5 Sistema de Registo de Produtos baseado em Blockchain

Este capítulo consiste na explicação da componente prática requerida para esta dissertação. São aplicados e explicados os processos teóricos necessários para a sua realização.

Para a realização do protótipo existiram várias dificuldades, visto requerer um maior nível de complexidade, originando, de igual modo, algumas modificações à medida que se foi desenvolvendo. No entanto, foi pretendido que o protótipo seguisse, à risca, a fundamentação teórica.

5.1 Perfil do Utilizador

Num sistema de registo de produtos, existem várias partes envolventes, como observado anteriormente. Para este projeto, pretendeu-se criar um utilizador, que foi quem serviu a etapa da "Manufatura". Um utilizador pode autenticar-se, registar um produto e submetê-lo e, posteriormente, visualizá-lo. Após submeter o produto, este será encaminhado para a Blockchain, onde será devidamente tratado e validado.

Para o protótipo, o pressuposto foi criar uma base de dados para os utilizadores e uma para os produtos registados. Na base de dados dos utilizadores, guardou-se a seguinte informação: nome e password. Na base de dados dos produtos, constam os seguintes dados: nome do fabricante, id do produto, nome do produto, local de fabrico, data de fabrico, data de expiração de validade, preço de produção e tipo de produto (ex.: fruta, vegetais, peixe, etc.). A divisão das bases de dados serve o pressuposto de transparência, segurança e confiabilidade.

Sucintamente, o perfil do utilizador contém nome e password e pode pesquisar por produtos já registados, através do id do produto pretendido. Nos seguintes pontos, serão aprofundados estes aspetos.

5.2 Autenticação e Autorização do Utilizador

Na autenticação e autorização, o utilizador terá de fornecer nome e password para se registar no sistema. De seguida, fará o login, onde a API irá consultar a base de dados, verificar se o nome consta na base de dados e se corresponde à password encriptada. A API, então, cria um token, que foi gerado com base numa chave secreta apenas conhecida pela API. Esse token é enviado de volta ao utilizador em forma de cookie, autorizando o utilizador a aceder ao sistema, enviando, posteriormente, à API com o intuito de garantir a autenticidade e integridade do utilizador.

Os tokens são criados através de algoritmos de *hash*, sendo impossível replicá-los. Para melhorar a segurança do sistema, a chave secreta, utilizada para gerar os tokens tem tempo limite até expirar, sendo automaticamente regenerada.

5.3 Arquitetura da Rede

Como já analisado, a *Blockchain* é uma rede descentralizada, que apresenta nós ligados entre si, formando uma rede *Peer-to-Peer* (P2P). Por isso, a *Blockchain* consegue fornecer segurança, integridade e não repúdio dos dados à aplicação a que for associada.

Numa *Blockchain* de criptomoedas, qualquer um pode ser um nó passível de minerar uma criptomoeda, o que garante segurança elevada e os mineradores podem receber incentivos monetários. No entanto, para um sistema de produção, propõe-se outra solução para a implementação, mas pretende-se manter a escalabilidade, segurança e bom desempenho.

A arquitetura de rede deste sistema será constituída por:

- **Manufatores** – atores passivos do sistema. Necessitam de se autenticar, com nome de utilizador e password, para acederem ao site e poderem registar produtos.
- ***Master Node*** – nó da rede que vai receber os produtos registados, transformá-los em blocos e encaminhá-los para o resto da rede.
- ***Validator Node*** – irá efetuar o processo de validação dos blocos, utilizando o algoritmo de consenso mais apropriado ao sistema, e adicionar os blocos à *Blockchain*.

A presença do ***Master Node*** é crucial para manter a integridade dos nós validadores. Por isso, irá escolher, aleatoriamente, qual o nó que será o validador para cada bloco.

O ***Master Node*** requer uma API (*Application Programming Interface*) associada a uma webapp. Essa API servirá o proposto da autenticação dos utilizadores, para poderem registar os seus produtos. Assim que os produtos são registados, são enviados para o *Master Node* e, posteriormente, para os restantes nós constituintes da rede.

Com o intuito de validar os produtos, utiliza-se um algoritmo de consenso que seja apropriado neste tipo de sistema. Mais adiante, veremos porque é que o *Proof of Stake* é o ideal.

Assim, teremos uma rede que transmite transparência, integridade, segurança e não repúdio dos dados, sendo os dados os produtos registados.

5.4 Segurança da Rede

Manter a segurança da rede é um passo muito importante a ter em conta. Por isso, no sistema, deve-se garantir a integridade dos nós participantes da rede que irão validar os produtos registados, escolhendo os que realizarão essa tarefa através do algoritmo de consenso.

Outra forma de transmitir segurança, será encriptar as passwords de cada utilizador. Do lado da rede *Blockchain*, as *hashes* serão responsáveis por manter a segurança, integridade e não repúdio dos dados.

5.5 Formação dos Blocos

Como já mencionado, uma *Blockchain* consiste em blocos ligados entre si. Esses blocos estão ligados através de uma assinatura digital, denominada *hash*. Uma *hash* é a transformação de um input de tamanho variável num output de tamanho fixo e é impossível voltar à *hash* original, tornando-a segura.

Para a assinatura digital, escolheu-se o algoritmo de *hashing* SHA-256, que já foi mencionado e explicado. Um algoritmo de *hashing* não deve ser muito rápido, porque pode originar colisões, nem muito lento, visto que pode prejudicar a eficiência de mitigação de problemas.

5.6 Proposta de Resolução do Sistema

Como já referido, o sistema será constituído por 3 nós importantes. Uma API, para autenticar e autorizar um utilizador e para reencaminhar os produtos registados para o próximo nó. O *Master Node*, tem como função distribuir os blocos formados pelos produtos para o próximo e último nó. O *Validator Node*, será responsável pelo algoritmo de consenso PoS, para validar esses blocos. Assim que o bloco é validado, é enviado de volta ao *Master Node*, sendo inserido na *Blockchain*.

A solução que se propõe para o lado do utilizador, é:

- O utilizador autentica-se com os seus dados, o seu acesso é autorizado, recebe o formulário para registar o seu produto e regista o produto.

Para o sistema, foram feitas várias pesquisas para determinar a melhor forma de o desenvolver, como estipulado na Metodologia. Sendo assim, para o desenvolvimento do sistema foram utilizadas as seguintes tecnologias:

- ***JavaScript*** – linguagem de programação utilizada para desenvolver a webapp e a *Blockchain*. Escolheu-se esta linguagem, por ser orientada a objetos, apoiar a

programação funcional, ser baseada em protótipo e por facilitar a comunicação e ocorrência de ações assíncronas, em simultâneo.

- **Node.js** – framework de javascript, importante para criar uma API. Possibilita a um utilizador autenticar-se e possui acesso direto à base de dados, onde serão armazenados os utilizadores e produtos.
- **HTML e CSS** – utilizados para o design do site, que permitirá a um utilizador autenticar-se e registar produtos. Também se utilizou o *Bootstrap*, que é uma framework de CSS, que visa atribuir um design mais fluído ao website.
- **MySQL** – base de dados relacional, do tipo SQL. Contém os dados dos utilizadores, que se autenticaram e, também, os dados dos produtos registados.

5.7 Desenvolvimento do Protótipo

Neste capítulo, será definido como se pretende desenvolver este protótipo em termos práticos, já tendo em conta as linguagens que se pretende utilizar e como se pretende que o website e a *Blockchain* funcionem.

5.7.1 Análise de Requisitos

De modo a construir este sistema, primeiro é necessário definir os requisitos funcionais e não-funcionais. Onde os funcionais são os que ditam as tarefas que o sistema deve realizar e os não-funcionais ditam como essas tarefas serão realizadas.

Os requisitos funcionais essenciais para o protótipo são os seguintes:

- O utilizador deve autenticar-se de forma segura;
- O sistema deve ser transparente ao utilizador;
- O sistema deve garantir a integridade dos dados;
- A rede deve implementar um algoritmo de consenso *Proof of Stake*.

Os requisitos não-funcionais são:

- Um utilizador regista-se com nome e password;
- A API autentica um utilizador de acordo com os dados que constam na base de dados;
- Na Blockchain, dá-se a validação de produtos, através do *Proof of Stake*;
- Assim que os produtos são validados, toda a rede toma conhecimento, de forma a garantir segurança e integridade.

Com isto, também se torna necessário desenvolver diagramas, para facilitar o desenvolvimento do protótipo, como:

- Diagrama de Casos de Uso;
- Diagrama de Classes (Rede *Blockchain*);
- Diagrama de Atividades;
- Diagrama de Sequência.

5.7.2 Diagrama de Casos de Uso

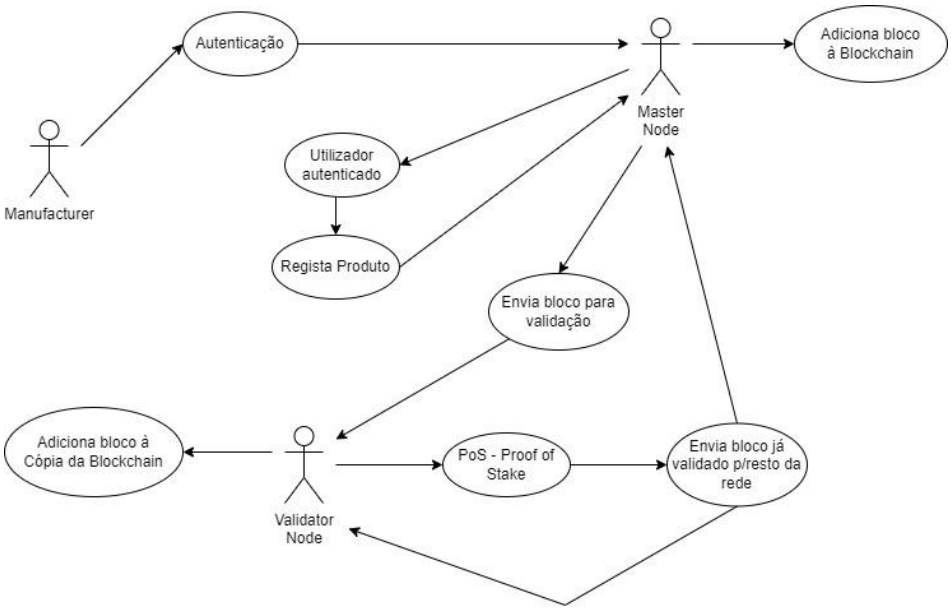

Figura 11 - Diagrama de Casos de Uso

O diagrama da Figura 11, que foi desenvolvido com o auxílio do diagrama de Casos de Uso em [32], mostra o raciocínio de como se idealizou o desenvolvimento prático da rede *Blockchain*, tendo em conta a fundamentação teórica. Um *Manufacturer* autentica-se de modo a poder registar produtos. A restante atividade pertencerá à rede *Blockchain*. Após o registo, o produto é encaminhado pela rede *Blockchain*.

Na rede, o produto é transformado em bloco e validado por um validador aleatório, escolhido pelo método de consenso *Proof of Stake*. Assim que um bloco é validado, é adicionado à *Blockchain*.

5.7.3 Diagrama de Classes (Rede *Blockchain*)

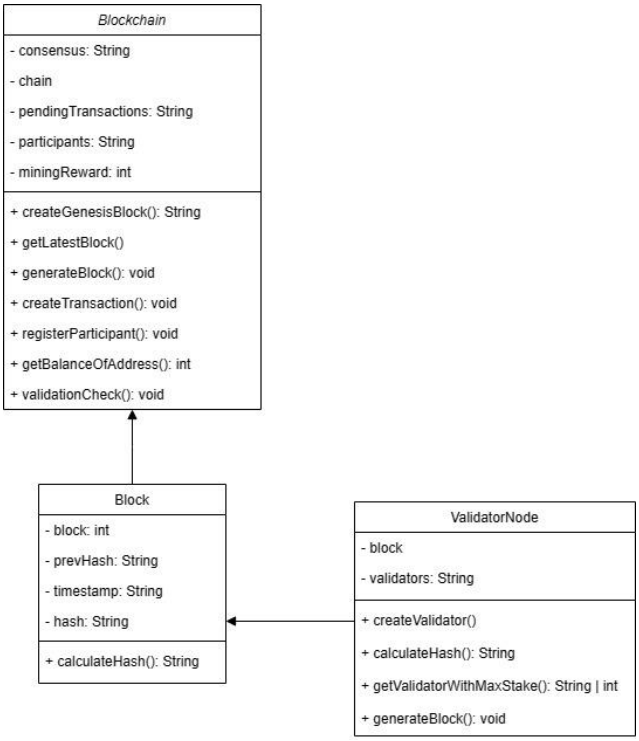

Figura 12 - Diagrama de Classes (Rede Blockchain)

Na Figura 12, é possível observar um diagrama de classes que demonstra como foi visualizada a implementação da rede *Blockchain*, de uma forma simplificada. A classe *Block* representa cada bloco de produtos, que será validado pela rede e será inserido na *Blockchain*. A classe *ValidatorNode* representa os nós que irão, através do algoritmo de consenso *Proof of Stake*, validar cada bloco, para poder ser armazenado na *Blockchain*. E, por fim, a classe *Blockchain*, que representa o local onde os blocos serão armazenados, só após validação.

5.7.4 Diagrama de Atividades

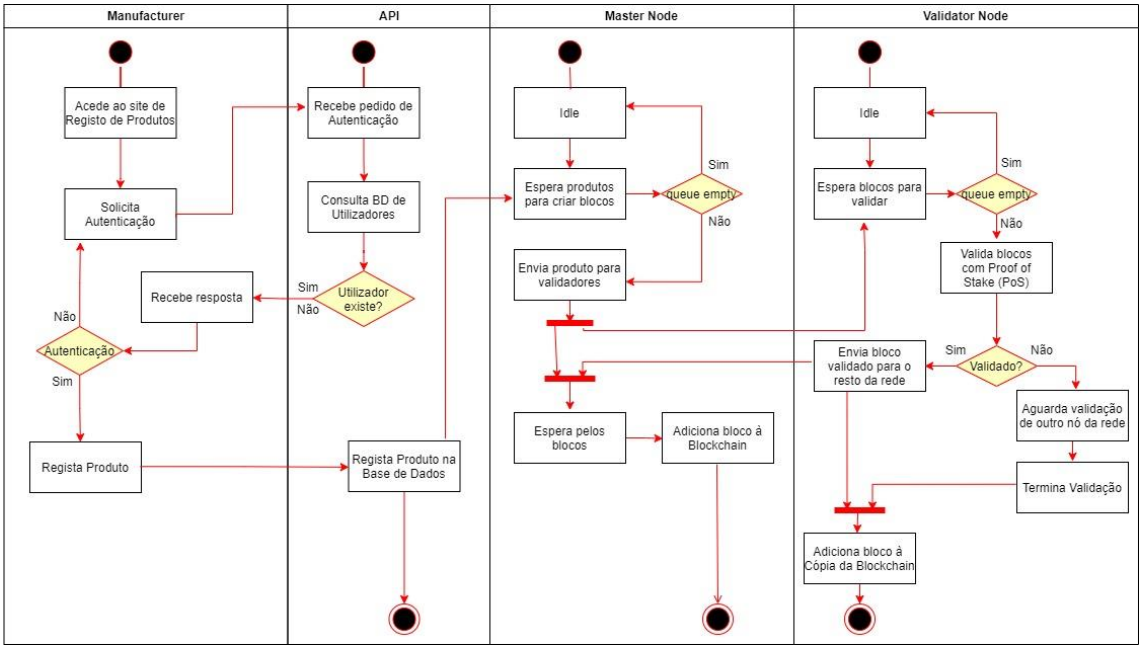

Figura 13 - Diagrama de Atividades

A Figura 13, demonstra um diagrama de atividades, que segue uma ordem de leitura cima para baixo, esquerda para direita. Por tal, o sistema começa no *Manufacturer*, com autenticação. De seguida, a API verifica as credenciais e autoriza ou não o utilizador, caso não autorize, o utilizador deve autenticar-se novamente, se autorizar, o utilizador regista o seu produto, que é guardado numa base de dados e é encaminhado para a rede *Blockchain*.

Na rede *Blockchain*, o *Master Node* recebe o produto e transforma-o em bloco, envia-o para validação, realizada por nós validadores aleatórios, que, tal como mencionado anteriormente, são decididos por *Proof of Stake*. Após validação, o bloco será adicionado à *Blockchain*.

5.7.5 Diagrama de Sequência

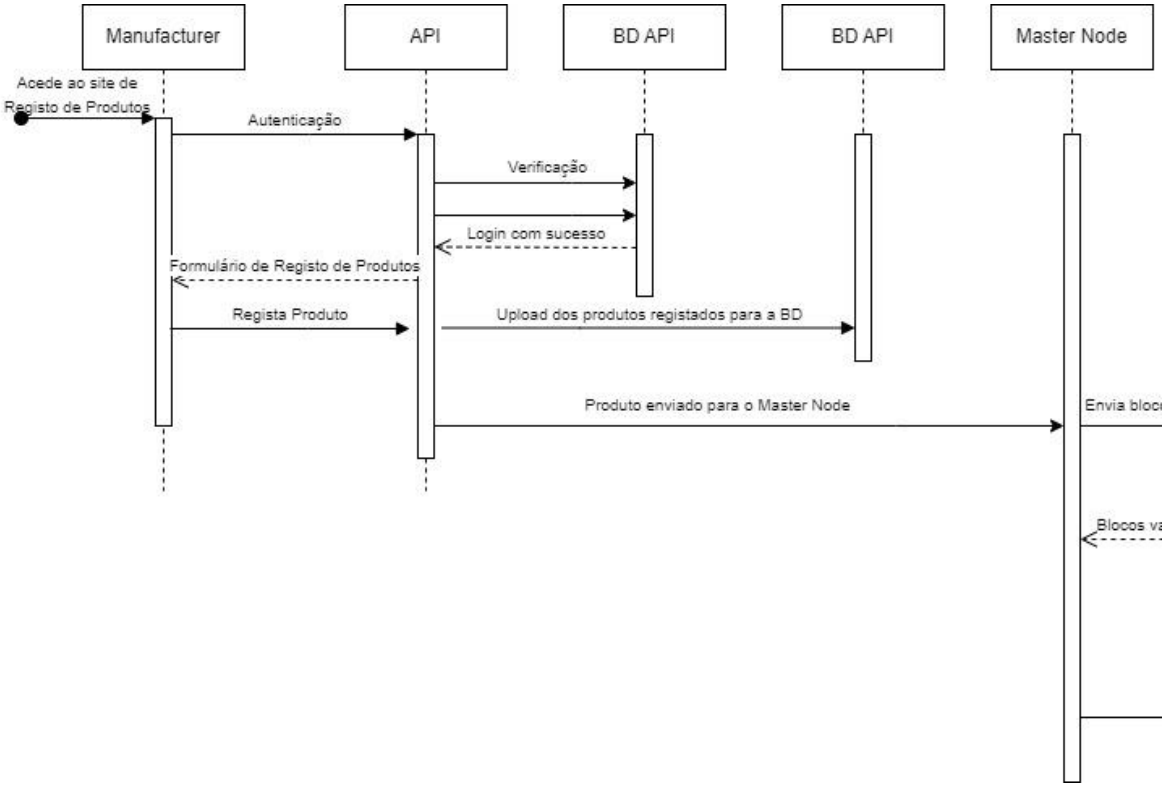

Figura 14 - Diagrama de Sequência (Parte 1)

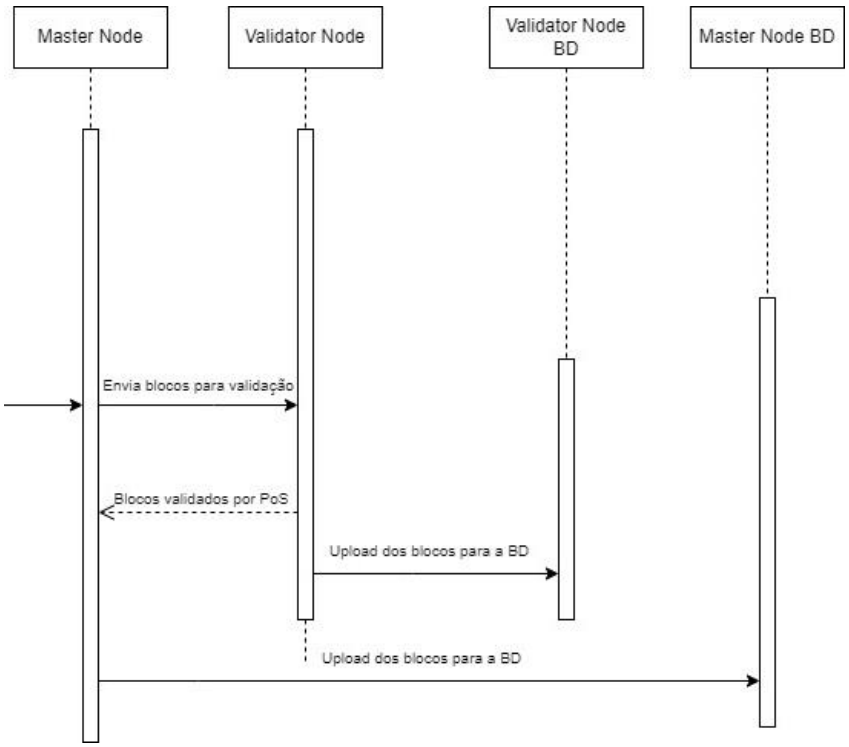

Figura 15 - Diagrama de Sequência (Parte 2)

Para facilitar ainda mais a compreensão do sistema, recorreu-se, de igual modo, ao desenvolvimento de um diagrama de sequência, ilustrado na Figura 14 e na Figura 15. Este

diagrama segue a mesma lógica que o de atividades, no entanto, a informação está mais simples de entender e demonstra a integração das bases de dados, na rede.

5.7.6 Website e API

Após definir as linguagens de programação a serem utilizadas, começou-se por desenvolver o website, visto ser a parte mais rápida e simples a desenvolver.

No desenvolvimento da API, criou-se um processo simples de autorização e autenticação, onde os utilizadores se registam com os seus dados (nome e password) e fazem login com esses mesmos dados. Assim, só utilizadores autenticados e autorizados é que podem registar produtos.

Toda a informação, desde dados dos utilizadores a dados dos produtos, é armazenada em bases de dados. As *passwords* dos utilizadores são guardadas na base de dados, encriptadas por um algoritmo de *hashing* e com um *salt*. O *salt* fornece maior segurança, por tornar as passwords mais robustas.

No website, um utilizador deve registar-se para poder registar os seus produtos e visualizá-los, posteriormente. Pretendeu-se desenvolver um site que demonstrasse facilidade e simplicidade aos utilizadores que tivesse, no entanto, a segurança provida da rede *Blockchain*. De seguida, estão apresentados exemplos: da página de *signup* e *login* de utilizador (Figura 16), da página de registo de produtos (Figura 17), da página de pesquisa de produtos (Figura 18), que inclui a tabela de produtos registados (Figura 19), servindo para demonstrar como os produtos devem ser apresentados num site funcional, futuro, e a página de criação de códigos QR (Figura 20).

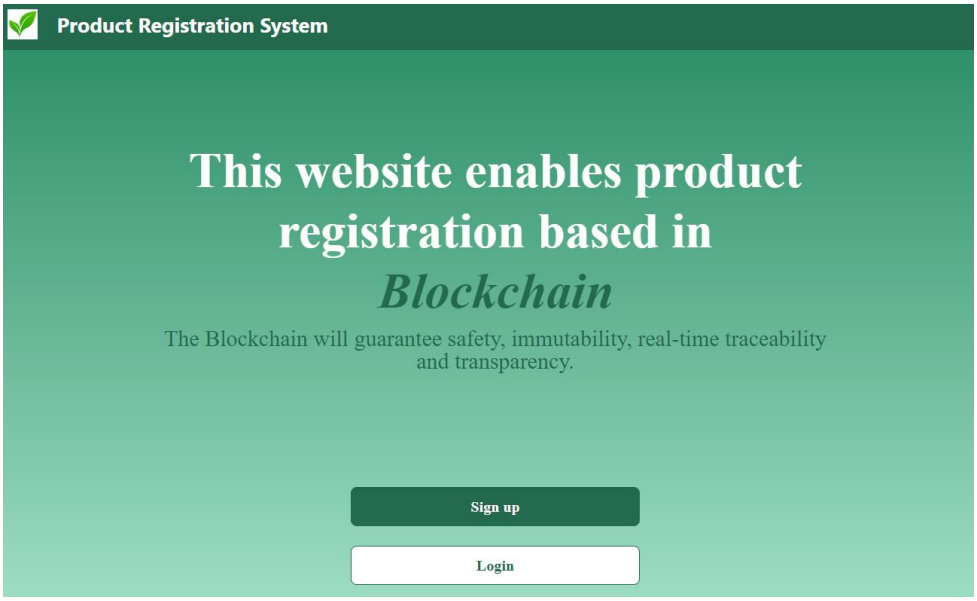

Figura 16 - Página de Registo de Utilizadores

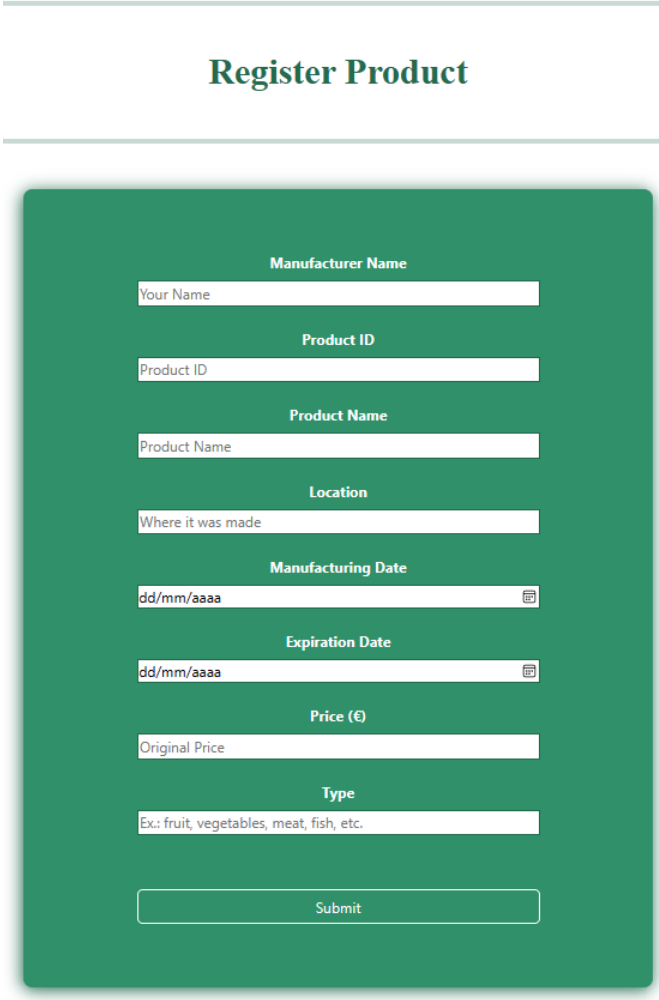

Figura 17 - Página de Registo de Produtos

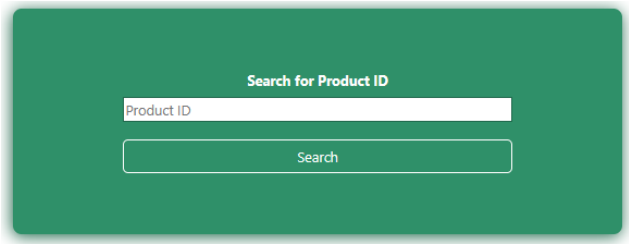

Figura 18 - Página de Pesquisa de Produtos

Product ID	Manufacturer Name	Product Name	Location	Manufacturing Date	Expiration Date	Price (€)	Type
1001	ines	chicken	sintra	2023-03-15	2023-04-15	16.00	meat
1002	danilson	cheese	sintra	2023-03-28	2023-04-28	2.00	dairy
1003	miguel	rice	coimbra	2023-04-03	2023-06-24	1.50	cereal
1004	joana	salmon	oslo	2023-03-24	2023-04-04	11.00	fish
1005	maria	potatoes	hauts-de-france	2023-05-10	2024-05-10	1.67	vegetable
1006	maria	eggs	florida	2023-05-03	2023-05-03	2.00	animal
1007	ricardo	milk	glasgow	2023-05-10	2023-05-25	1.20	dairy
1008	ricardo	sea bass	helsinky	2023-05-10	2023-05-14	16.00	meat

Figura 19 - Tabela de Produtos

Figura 20 - Página de Criação de Códigos QR

5.7.7 Estrutura da Rede *Blockchain*

Este capítulo tem em conta as pesquisas feitas para o desenvolvimento da rede *Blockchain*. Nessas pesquisas, pretendeu-se entender o que requer a *Blockchain*, em termos práticos.

Observou-se que uma *Blockchain*, no geral, requer blocos, cada constituído por timestamp, *hash*, informação do bloco e *previous hash*, isto é, a *hash* do bloco anterior, requer a adição de novos blocos e requer um algoritmo de consenso. Com isto, seguiu-se para a decisão de qual algoritmo de consenso seria o mais ideal para este protótipo. Após algumas pesquisas, reduziu-se o número de algoritmos de consenso para dois, o *Proof of Stake* (PoS) e o *Proof of Authority* (PoA).

O PoS pretende validar os blocos de transações da rede, através do investimento monetário de cada utilizador, podendo, posteriormente, receber uma recompensa pela sua cooperação. A escolha de validador é feita aleatoriamente, demonstrando igualdade com todos os validadores.

O PoA pretende validar os blocos de transações da rede, através de validadores autorizados, que investem a sua reputação, ao invés de dinheiro. Este algoritmo aproxima-se de um sistema mais centralizado que o PoS.

Visto que o *Proof of Authority* se demonstra um algoritmo de consenso mais centralizado, optou-se pelo *Proof of Stake*.

5.7.7.1 Bloco Genesis

Na Figura 21, está representado o bloco genesis, ou seja, o primeiro bloco que se criou para dar início à *Blockchain*. Este bloco é constituído por "*block*", isto é, o número ou índice do bloco, "*prevHash*", indicada como 0, visto que não existe nenhum bloco anterior,

"*timestamp*", demonstra a data quando foi criado (indicada pelo programador), "*transactions*", representa a informação do bloco e "*hash*", criada a partir da assinatura digital, do algoritmo de *hashing* SHA-256.

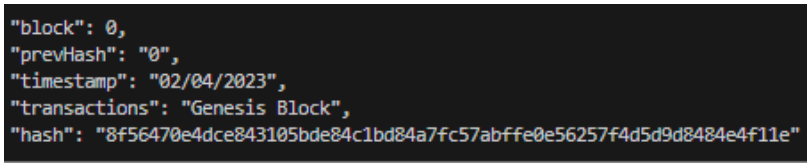

Figura 21 - Bloco Genesis

5.7.7.2 Exemplo de Bloco

Pela Figura 22, pode-se visualizar um exemplo de um bloco criado a partir do produto registado. Este bloco possui as mesmas variáveis que o anterior, com a adição do "*validator*", que representa o nó que está a validar o bloco, que veremos mais adiante como é escolhido. A informação do bloco provém dos atributos definidos para o registo do produto, mais os atributos dos endereços de onde é produzido e para onde é enviado, e o atributo "*amount*", que contém a quantidade do produto a ser enviado.

Figura 22 - Exemplo de Bloco

5.7.7.3 Validadores

Um validador é decidido a partir do algoritmo de consenso *Proof of Stake*, que, como indica a teoria, um validador deve investir do seu próprio dinheiro, de modo a poder ser um validador e quanto mais investir, maior a probabilidade de ser escolhido. Podemos observar pela Figura 23, como se realizou esta implementação, que serve apenas para demonstração. Onde se seleciona o nó validador que tiver investido mais, através do "*maxStake*".

```
getValidatorWithMaxStake() {
    let maxStake = ["", 0];
    this.validators.forEach(function(element) {
        if (element[1] > maxStake[1]) {
            maxStake = element;
        }
    });
    return maxStake;
}
```

Figura 23 - Escolha de Validador através de Proof of Stake

5.8 Dificuldades sentidas

Com o desenvolvimento deste protótipo, existiram várias dificuldades, algumas ultrapassadas e outras mantiveram-se. Dificuldades de estruturação da rede, como manter integridade e segurança, etc.

O desafio principal foi determinar como se poderia estruturar a rede, quais seriam os agentes da *Blockchain*, como iriam operar, qual seria o método de validação a utilizar e como funcionaria. Sendo assim, o desenvolvimento da rede demorou mais do que o que se esperava. No entanto, os diagramas facilitaram o raciocínio, a identificação do problema e o modo de como seria mitigado.

Uma dificuldade não ultrapassada foi realizar a comunicação ponto-a-ponto, de modo que os produtos fossem enviados automaticamente para a rede *Blockchain*, logos após serem registados.

5.9 Manual de Instalação

Neste manual será explicado o processo para executar o site e a *Blockchain*. Será necessário utilizar o VS Code e o MySQL *Workbench*.

Primeiro, devem-se importar o ficheiro "*WebApp*", no VS Code e a pasta "*databases*", no MySQL *Workbench*. Nos capítulos seguintes será demonstrado como importar e executá-los, para os ver a funcionar corretamente.

5.9.1 Importar Base de Dados "*databases*" (MySQL *Workbench*)

Para importar a base de dados, é necessário ter o MySQL *Workbench* instalado. No servidor selecionar a opção para importar, como demonstra a Figura 24. Depois, seleciona-se a opção "*Import from Dump Project Folder*" e escolhe-se o caminho onde se encontra a pasta (Figura 25). Clica-se em "*Import Progress*" (Figura 26) e em "*Start Import*".

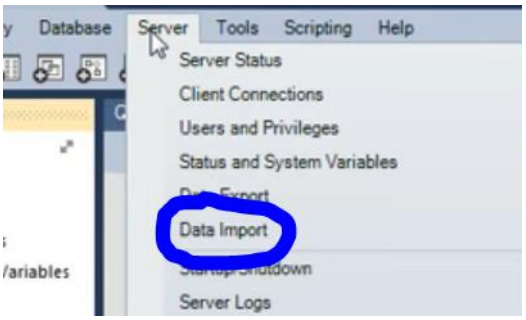

Figura 24 - Importar Base de Dados

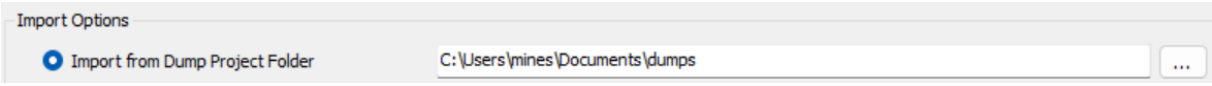

Figura 25 - Importar pasta

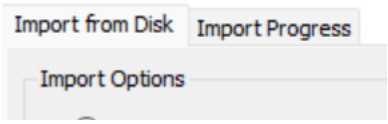

Figura 26 - "Import Progress"

Após importar a pasta, as bases de dados irão aparecer no "*Schemas*" (Figura 27), se não aparecer automaticamente, deve-se carregar no *refresh* do lado direito do "*Schemas*". Por fim, para mostrar as tabelas, clica-se no ícone ilustrado na Figura 28.

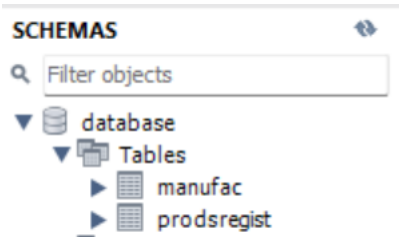

Figura 27 - "Schemas"

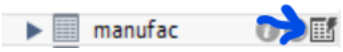

Figura 28 - Mostrar tabela

5.9.2 Alterações necessárias no VS Code

Para visualizar as bases de dados a funcionar, quando cria um utilizador, é necessário alterar a linha 8 no ficheiro mysql.js, como mostra a Figura 29, para a sua rota, "mysql://root:<SuaPassword>@localhost:3306/database". No caso de o PORT ser diferente do 3306, deve alterá-lo, também. Se os dados dos utilizadores ou dos produtos não aparecerem automaticamente, basta fazer *refresh*.

De modo a poder utilizar o site e as bases de dados, também é necessário instalar alguns pacotes, através do seguinte comando: npm install, que irá instalar todas as dependências requeridas pelo projeto.

```
8                   .createConnection('mysql://root:Mp1Rp2D%@localhost:3306/database') //Switch to the mysql workbench route
```

Figura 29 - Linha a ser alterada

Para poder utilizar o site, deve introduzir no terminal o comando: node server.js. Para visualizar a rede *Blockchain*, deve introduzir o comando: node BlockchainNetwork.js.

Se pretender adicionar um bloco à *Blockchain*, deve adicionar código no ficheiro BlockchainNetwork.js. Nas Figura 30 e Figura 31, é demonstrado um exemplo de bloco a ser criado e a sua transação, respetivamente, com o intuito de auxiliar a adição de novos blocos.

```
124   // Block 8
125   console.log("-".repeat(repeat_lines))
126   console.log('Creating Block 8...');
127   console.log('\nChoosing validator...');
128   validator = proofofstake.getValidatorWithMaxStake()[0];
129   console.log("Validator with the highest stake chosen: " + validator);
130
131   blockchain.generateBlock(validator);
132   console.log('\nMiner of Block 7 has been rewarded...');
```

Figura 30 - Criar bloco

```
119   //added transaction
120   console.log('-'.repeat(repeat_lines));
121   console.log('\nNew Transactions created...');
122   blockchain.createTransaction(new Transaction(Participants.accounts()[0][0], Participants.accounts()[1][0], 'ricardo', 1007, 'milk',
```

Figura 31 - Adicionar transação

Na Figura 30, pode-se observar um bloco, denominado “Bloco 8”, a ser criado, onde se escolhe um validador, de acordo com o algoritmo *Proof of Stake*, e, posteriormente, se valida o bloco anterior, pois se não for validado, não será visível. Na Figura 31, é possível observar uma transação criada e associada ao bloco, que corresponde às variáveis requeridas para cada nova transação. Por isso, sempre que seja necessário adicionar um novo bloco, devem-se colocar os aspetos apresentados acima.

Com isto, já se pode visualizar o site, as bases de dados e a rede *Blockchain*, a funcionar corretamente.

5.10 Manual de Utilizador

Neste manual pretende-se instruir o utilizador a fazer uso da webapp, desde o registo de utilizador até ao logoff. De seguida irá demonstrar-se cada página do website e como navegar nele.

Primeiro, um utilizador deve registar-se, clicando no botão "*Sign up*", fazendo aparecer o formulário da Figura 32. Após registo, poderá clicar no botão "*Login*", aparecendo o formulário da Figura 33.

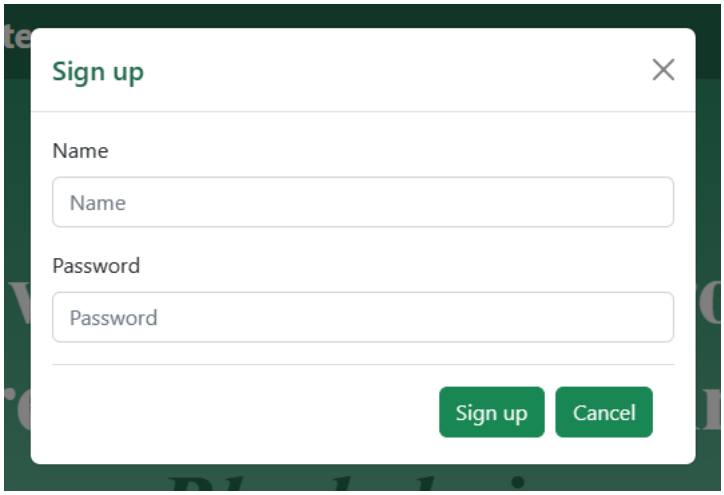

Figura 32 - Formulário de Registo de Utilizador

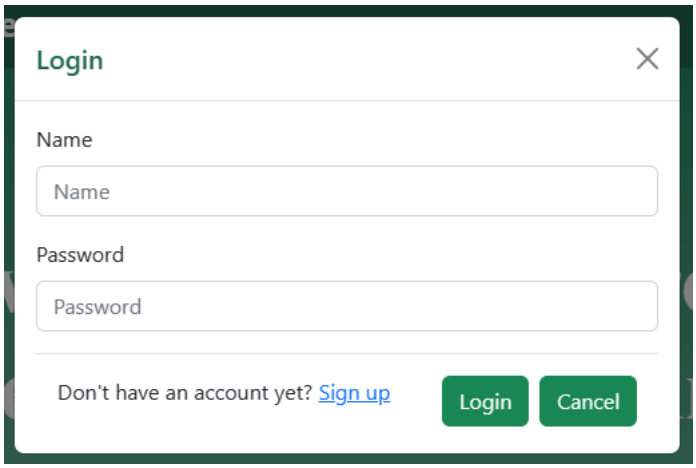

Figura 33 - Formulário de Login de Utilizador

Assim que é autorizado a navegar no site, irá surgir o formulário para registar produtos, apenas sendo necessário seguir os requisitos lá estipulados, como demonstra a Figura 17. Após registar os seus produtos, poderá visualizá-los, gerar código QR ou fazer *logoff*, que se encontram no canto superior direito da página de registos de produtos, como demonstra a Figura 34.

Figura 34 - Opções para ver outras páginas

Se escolher a opção "*Search*", surgirá uma caixa para procurar os seus produtos e uma tabela onde estarão todos os produtos, como ilustram as Figura 18 e Figura 19, respetivamente. No entanto, ambos servem só para demonstração, não estando funcionais.

Se escolher a opção "*Generate QR Code*", surgirá uma caixa a solicitar o nome do produto para o qual pretende criar um código QR, como demonstra a Figura 20.

No caso de escolher a opção "*Logoff*", será redirecionado para a página inicial, podendo realizar, novamente, login ou registar um novo utilizador.

6 Conclusões

Com esta dissertação, foi possível conhecer mais aprofundadamente uma rede *Blockchain* e uma cadeia de abastecimento, o que envolvem ambas, como funcionam, tanto em teoria como em prática. Pode-se concluir que, realmente, a *Blockchain* é uma rede bastante complexa, como se viu tanto numa análise teórica como prática, sendo, consequentemente, uma rede segura e confiável.

Ao associar uma rede *Blockchain* a uma Cadeia de Abastecimento, é possível fornecer maior segurança, autonomia, rastreamento em tempo real e transparência, que é bastante importante para a tradução de confiança aos consumidores e, também, para garantir qualidade e valor do produto.

Verificou-se que o rastreamento funciona melhor se associado a uma rede descentralizada, por esta dificultar a manipulação de dados, evitar o ponto único de falha, que surge na abordagem centralizada, e por ser mais rápida e eficiente na tomada de decisões.

Para uma empresa ter sucesso, o mais importante é transmitir confiança aos seus consumidores, através da transparência, da adoção de princípios sustentáveis e do apoio à comunidade, garantindo um impacto positivo nela.

Com o desenvolvimento do protótipo, conseguiu confirmar-se a garantia da segurança disponibilizada, tanto para a API como para a rede *Blockchain*, tal como pretendido. Na API, o utilizador deve autenticar-se, de modo a utilizar o site e a sua password é encriptada. Isto mantém a segurança do website e protege o utilizador contra ataques maliciosos. Na rede *Blockchain*, as *hashes* e o facto de a rede exigir integridade dos nós participantes, também ajuda a manter a segurança, visto que, as hashes usam criptografia e os nós validadores só são autorizados a validar um bloco, se forem escolhidos pelo algoritmo de consenso. Isto demonstra que a *Blockchain* pode ser uma boa opção para registar produtos e, possivelmente, para rastreá-los ao longo da cadeia de abastecimento. No entanto, será necessário realizar a integração das restantes etapas da SCM (Planeamento, Abastecimento, Entrega e Devolução), na prática, para chegar a tais conclusões.

7 Sugestões para Trabalhos Futuros

Com o desenvolvimento prático desta dissertação existiram alguns aspetos que necessitam de melhoria e aspetos que ainda precisam de ser realizados.

Como estipulado nas dificuldades sentidas (5.8), não se conseguiu ligar a API à *Blockchain*, sendo que os produtos não estão a ser enviados automaticamente para a rede *Blockchain*. Este é um aspeto a ser estudado e implementado para permitir comunicação ponto-a-ponto. Por outro lado, resta acrescentar as outras etapas da cadeia de abastecimento, isto é, Planeamento, Abastecimento, Entrega e Devolução, com o intuito de deixar de ser só um protótipo e possibilitar conclusões mais concretas à cerca das vantagens da Blockchain num Sistema de Registo de Produtos e como a tecnologia pode melhorar o rastreamento de produtos. Estes são dois pontos que não se conseguiu realizar.

Visto que ainda é um protótipo, muitos aspetos servem apenas para teste. Por isso, de seguida são demonstradas algumas melhorias a realizar:

- No registo de produtos, deve ter requisitos mais específicos para cada tipo de produto, para demonstrar maior transparência e ganhar confiança dos consumidores;
- Na procura de produtos, a tabela deve receber os produtos automaticamente após submissão dos mesmos e deve ser possível pesquisar os produtos presentes na tabela;
- Na página para criar QR Codes, terá de ser possível mostrar a informação toda do produto;

Quanto ao desenvolvimento da parte teórica, pretende-se que as pesquisas realizadas auxiliem trabalhos futuros, de modo a também originar atualizações e melhorias na tecnologia *Blockchain*, visto que ainda é algo relativamente recente e será uma tecnologia potencialmente usada na Web 3.0.

8 Bibliografia

[1] wikipedia, “Blockchain,” Wikipedia The Free Encyclopedia, 24 October 2022. [Online]. Available: https://en.wikipedia.org/wiki/Blockchain. [Accessed 25 October 2022].

[2] M. M. d. Silva, “Blockchain do Bitcoin: Perspetivas de Utilização Massivas noutras Áreas,” Universidade Autónoma de Lisboa, 21 February 2022. [Online]. Available: https://www.youtube.com/watch?v=vSSyknWB0ns. [Accessed 10 October 2022].

[3] R. Sheldon, “A timeline and history of blockchain technology,” TechTarget, 9 August 2021. [Online]. Available: https://www.techtarget.com/whatis/feature/A-timeline-and-history-of-blockchain-technology. [Accessed 20 October 2022].

[4] C. Jaikaran, “Beyond Bitcoin: Emerging Applications for Blockchain Technology,” Congressional Research Service, 2018.

[5] S. Daley, “34 Blockchain Applications and Real-World Use Cases,” builtin, August 2022. [Online]. Available: https://builtin.com/blockchain/blockchain-applications. [Accessed 21 October 2022].

[6] wikipedia, “Gestão da cadeia de suprimentos,” Wikipédia, a enciclopédia livre, 27 May 2019. [Online]. Available: https://pt.wikipedia.org/wiki/Gest%C3%A3o_da_cadeia_de_suprimentos. [Accessed 7 November 2022].

[7] W. Viriyasitavat, L. D. Xu, Z. Bi and A. Sapsomboon, *Blockchain-based business process management (BPM) framework for service composition in industry 4.0*, *Journal of Intelligent Manufacturing,* vol. 31, no. 7, pp. 1737-1748, 2020, doi: 10.1007/s10845-018-1422-y.

[8] F. Yiannas, “Walmart's food safety solution using IBM Food Trust built on the IBM Blockchain Platform,” IBM Blockchain, 22 August 2017. [Online]. Available: https://www.youtube.com/watch?v=SV0KXBxSoio. [Accessed 25 October 2022].

[9] A. Abrol, “Decentralized Vs. Centralized: A detailed comparison,” Blockchain Council, 5 September 2022. [Online]. Available: https://www.blockchain-council.org/blockchain/decentralized-vs-centralized/. [Accessed 23 November 2022].

[10] “What is Bitcoin?,” WeUseCoins, 24 April 2014. [Online]. Available: https://www.youtube.com/watch?v=Gc2en3nHxA4&t=17s. [Accessed 25 October 2022].

[11] “How do Bitcoin Transactions Work?,” River Financial, [Online]. Available: https://river.com/learn/how-does-a-bitcoin-transaction-work/. [Accessed 25 October 2022].

[12] E. Hong, “How does Bitcoin Mining work?,” Investopedia, 05 May 2022. [Online]. Available: https://www.investopedia.com/tech/how-does-bitcoin-mining-work/. [Accessed 27 October 2022].

[13] B. Baker, “What is Bitcoin mining and how does it work?,” Bankrate, 27 September 2022. [Online]. Available: https://www.bankrate.com/investing/what-is-bitcoin-mining/. [Accessed 27 October 2022].

[14] G. Gibert, G. Santos, J. Gibert and P. Cardoso, “Desenvolvimento de um protótipo de rede Blockchain para criptomoedas,” Universidade Autónoma de Lisboa, Lisboa, 2022.

[15] W. Vermaak, “What are Peer-to-Peer (P2P) Networks?,” coinmarketcap, 2021. [Online]. Available: https://coinmarketcap.com/alexandria/article/what-is-peer-to-peer-p2p. [Accessed 1 November 2022].

[16] S. Ohzahata and K. Kawashima, *An experimental study of peer behavior in a pure P2P network*, *Journal of Systems and Software,* vol. 84, no. 1, pp. 21-28, 2011, https://doi.org/10.1016/j.jss.2010.08.025.

[17] “Peer to Peer Network,” Teach Computer Science, [Online]. Available: https://teachcomputerscience.com/peer-to-peer-network/. [Accessed 1 November 2022].

[18] N. Kumar, “What are Peer-to-Peer (P2P) Networks?,” Enjoy Algorithms, 6 September 2021. [Online]. Available:

https://www.enjoyalgorithms.com/blog/peer-to-peer-networks. [Accessed 1 November 2022].

[19] "6 Major Features of Blockchain | Why Blockchain is Popular?," Data Flair, [Online]. Available: https://data-flair.training/blogs/features-of-blockchain/. [Accessed 15 November 2022].

[20] geeksforgeeks, "Blockchain Features," Geeks for Geeks, 24 May 2022. [Online]. Available: https://www.geeksforgeeks.org/features-of-blockchain/?tab=article. [Accessed 15 November 2022].

[21] "Benefits of Blockchain," IBM, [Online]. Available: https://www.ibm.com/topics/benefits-of-blockchain. [Accessed 15 November 2022].

[22] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," in *2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE),* Vilnius, 2018.

[23] C. Parizo, "What are the 4 different types of blockchain technology?," TechTarget, 28 May 2021. [Online]. Available: https://www.techtarget.com/searchcio/feature/What-are-the-4-different-types-of-blockchain-technology. [Accessed 8 November 2022].

[24] geeksforgeeks, "Types of Blockchain," Geeks for Geeks, 2 August 2022. [Online]. Available: https://www.geeksforgeeks.org/types-of-blockchain/. [Accessed 8 November 2022].

[25] geeksforgeeks, "Cryptography in Blockchain," Geeks for Geeks, 20 September 2022. [Online]. Available: https://www.geeksforgeeks.org/cryptography-in-blockchain/. [Accessed 20 November 2022].

[26] geeksforgeeks, "Difference between Private key and Public key," Geeks for Geeks, 8 June 2022. [Online]. Available: https://www.geeksforgeeks.org/difference-between-private-key-and-public-key/. [Accessed 20 November 2022].

[27] "Symmetric vs. Asymmetric Encryption - What are differences?," SSL2BUY, [Online]. Available: https://www.ssl2buy.com/wiki/symmetric-vs-asymmetric-encryption-what-are-differences. [Accessed 2022 November 20].

[28] NeuralNine, “Coding a Blockchain in Python,” Youtube, 14 March 2021. [Online]. Available: https://www.youtube.com/watch?v=pYasYyjByKI. [Accessed 22 November 2022].

[29] “Hashing Algorithm Overview: Types, Methodologies & Usage,” okta, [Online]. Available: https://www.okta.com/identity-101/hashing-algorithms/. [Accessed 22 November 2022].

[30] “What is the best Hashing Algorithm?,” Code Signing Store, [Online]. Available: https://codesigningstore.com/what-is-the-best-hashing-algorithm. [Accessed 22 November 2022].

[31] “SHA-256 hash calculator,” XORBIN, [Online]. Available: https://xorbin.com/tools/sha256-hash-calculator. [Accessed 22 November 2022].

[32] R. S. d. Pereira, “Sistema de Votação Digital baseado em Tecnologia Blockchain,” Universidade Autónoma de Lisboa, Lisboa, 2022.

[33] R. A. S., “Merkle Tree in Blockchain: What is it, How does it work and Benefits,” simplilear, 27 October 2022. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/merkle-tree-in-blockchain. [Accessed 26 November 2022].

[34] T. Kanstrén, “Merkle Trees: Concepts and Use Cases,” medium, 16 February 2021. [Online]. Available: https://medium.com/coinmonks/merkle-trees-concepts-and-use-cases-5da873702318. [Accessed 26 November 2022].

[35] geeksforgeeks, “Consensus Algoirthms in Blockchain,” Geeks for Geeks, 29 June 2022. [Online]. Available: https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/. [Accessed 9 November 2022].

[36] “How many Consensus Algorithms are There? An Overview,” originstamp, [Online]. Available: https://originstamp.com/blog/how-many-consensus-algorithms-are-there-an-overview/. [Accessed 9 November 2022].

[37] Z. Voell, “Bitcoin Mining Difficulty Hits Record High Amid Miner Revenue Surge,” CoinDesk, 9 January 2021. [Online]. Available: https://www.coindesk.com/markets/2021/01/09/bitcoin-mining-difficulty-hits-record-high-amid-miner-revenue-surge/. [Accessed 9 November 2022].

[38] Grace, “Delegated Proof of Stake (DPoS) Explained,” limechain, 29 September 2022. [Online]. Available: https://limechain.tech/blog/delegated-proof-of-stake-explained/. [Accessed 10 November 2022].

[39] “Proof of Authority Explained,” Binance Academy, 10 December 2020. [Online]. Available: https://academy.binance.com/en/articles/proof-of-authority-explained. [Accessed 10 November 2022].

[40] “Smart Contract Concepts and Practice,” Witscad, [Online]. Available: https://witscad.com/course/blockchain-fundamentals/chapter/smart-contract-concepts. [Accessed 27 November 2022].

[41] “What are Smart Contracts?,” Binance Academy, 23 September 2022. [Online]. Available: https://academy.binance.com/en/articles/what-are-smart-contracts. [Accessed 27 November 2022].

[42] G. Lawton, “Smart Contract,” techtarget, [Online]. Available: https://www.techtarget.com/searchcio/definition/smart-contract. [Accessed 27 November 2022].

[43] “What are smart contracts on blockchain?,” IBM, [Online]. Available: https://www.ibm.com/topics/smart-contracts. [Accessed 27 November 2022].

[44] Irawen, “Smart Contracts work in Blockchain,” [Online]. Available: https://www.ntirawen.com/2021/05/smart-contracts-work-in-blockchain.html. [Accessed 27 November 2022].

[45] “Smart contracts: contracts to formalise agreements in the digital age,” iberdrola, [Online]. Available: https://www.iberdrola.com/innovation/smart-contracts. [Accessed 27 November 2022].

[46] geeksforgeeks, “Smart Contracts and IoT,” Geeks for Geeks, 7 October 2022. [Online]. Available: https://www.geeksforgeeks.org/smart-contracts-and-iot/. [Accessed 27 November 2022].

[47] “Gestão de suprimentos,” fábricainfo, [Online]. Available: http://www.fabricainfo.com/servicos/gestao-de-suprimentos/. [Accessed 29 November 2022].

[48] T. Colaborador, “Gestão da cadeia de suprimentos ou SCM,” ComputerWeekly, [Online]. Available:

https://www.computerweekly.com/br/definicoe/Gestaodacadeiadesuprimentoso u-SCM. [Accessed 29 November 2022].

[49] M. M. d. Silva, “Support Technologies and future Trends of blockchain and Cryptocurrencies,” International Webinar on Blockchain & Cryptocurrencies, Universidade Autónoma de Lisboa, 24 May 2022. [Online]. Available: https://www.youtube.com/watch?v=eHnLZoopbiU. [Accessed 10 October 2022].

[50] J. Fernando, “Supply Chain Management (SCM): How it works and why it is important,” Investopedia, 7 July 2022. [Online]. Available: https://www.investopedia.com/terms/s/scm.asp#toc-what-is-supply-chain-management-scm. [Accessed 30 November 2022].

[51] “Managing risk in supply chains,” Queensland Government, 24 November 2022. [Online]. Available: https://www.business.qld.gov.au/running-business/suppliers-stock/supply-chains. [Accessed 1 December 2022].

[52] R. Dubey, A. Gunasekaran, T. Papadopoulos, S. J. Childe, K. T. Shibin and S. F. Wamba, *Sustainable supply chain management: framework and further research directions, J. Clean. Prod.*, vol. 142, pp. 1119-1130, 2017, doi: 10.1016/j.jelepro.2016.03.117.

[53] J. Sunny, N. Undralla and V. M. Pillai, *Supply chain transparency through blockchain-based traceability: An overview with demonstration*, *Computers & Industrial Engineering,* vol. 150, p. 106895, 2020, https://doi.org/10.1016/j.cie.2020.106895.

9 Apêndices

9.1 Cronograma

Atividades/Meses	Dez	Jan	Fev	Mar	Abr	Maio	Junho
Pesquisa prática sobre estudo de ferramentas para componente prática	**X**	**X**	**X**	**X**			
Desenvolvimento de uma rede Blockchain			**X**	**X**	**X**		
Desenvolvimento de um website			**X**	**X**	**X**		
Descrição das componentes práticas na Dissertação					**X**	**X**	
Entrega						**X**	
Revisão do Orientador						**X**	**X**
Preparação para defesa							**X**