ASSOCIAÇÃO DE POLITÉCNICOS DO NORTE (APNOR)

INSTITUTO POLITÉCNICO DE VIANA DO CASTELO

O PAPEL DAS CRIPTOMOEDAS E DA TECNOLOGIA BLOCKCHAIN NOS MERCADOS FINANCEIROS E OS SEUS EFEITOS NOS MEIOS DE PAGAMENTO

David Joel Gonçalves Oliveira

Dissertação apresentada ao Instituto Politécnico de Viana do Castelo para obtenção do Grau de Mestre em Gestão das Organizações, Ramo de Gestão de Empresas

Orientada por

Professor Doutor Nuno Domingues

Viana do Castelo, junho de 2023.

Resumo

O tema escolhido na dissertação para o Mestrado de Gestão das Organizações, ramo gestão de empresas é "A tecnologia *blockchain*, as criptomoedas e como podem alterar os meios de pagamento". Irá abordar-se o que é a *blockchain*, as várias criptomoedas que existem no mercado, os papeis que elas desempenham e poderão desempenhar no futuro.

Desde os tempos primordiais, que a necessidade de realizar transações é essencial para a vida em sociedade, para satisfazer as necessidades de comer, dormir, beber e outras mais secundárias, tais como comprar roupa, um telemóvel ou um computador. Para suprimir as necessidades, há uma troca de bens e serviços, em que o seu valor é definido pelo seu vendedor e terá de ser aceite pelo comprador, para haver transação comercial. Nos tempos primordiais, existia a troca direta de bens, dez galinhas por um porco, por exemplo.

Houve então a necessidade de evoluir e simplificar estes processos, com a inserção das moedas de bronze em 1.000 A.C na China. Posteriormente, foram utilizados materiais preciosos, como o ouro e prata para que as moedas tivessem um maior valor.

Mais tarde, houve a introdução da utilização do papel, como substituição das moedas, o que nos leva aos dias de hoje, em que fazemos pagamentos de várias formas, seja através de cartões de crédito, através de transferências bancárias, transferências de Paypal*, wearables* ou de telemóveis. Nos dias de hoje, começaram a generalizar-se os pagamentos com criptomoedas, tendo-se registado uma enorme evolução num curto espaço de tempo, das formas como realizamos transações e efetuamos pagamentos. Isto resulta do constante aumento tecnológico que assistimos nos dias de hoje, em que temos necessidade de facilitar as várias tarefas do quotidiano, sendo os pagamentos uma dessas tarefas mais correntes no dia a dia de cada pessoa.

De facto, verifica-se que os meios de pagamento tradicionais estão a tornar-se obsoletos, dando-se prioridade a pagamentos que não envolvam dinheiro físico (moedas e notas) optando-se pela utilização de cartões via "*Near Field Communication* "(NFC). Outra razão para isto estar a acontecer deve-se ao facto de termos vivido uma pandemia global, em que uma das formas do vírus se transmitir é por objetos que foram contactados por várias pessoas, como é o caso do dinheiro físico.

Foi realizada uma análise empírica com o objetivo de verificar a possível correlação entre a *Bitcoin*, a *Ethereum* e o índice *SP500*. O principal objetivo foi avaliar se há uma paridade potencial entre as criptomoedas (*Bitcoin* e *Ethereum*) e o índice *SP500*. A análise incluiu a investigação de seus comportamentos,

desempenhos e correlações ao longo do tempo, tentado identificar possíveis padrões ou correlações significativas. Os resultados mostraram que há uma correlação entre as criptomoedas devido à volatilidade que ambas compartilham. No entanto, não foi encontrada correlação entre as criptomoedas e o índice *SP500*.

Palavras-chaves: Criptomoedas; *Bitcoin*; *Blockchain*; Pagamentos; Tecnologia.

Abstract

The theme chosen for the dissertation to get the graduation of Master on Management of Organizations in the field of Business Management is "The role of blockchain technology, cryptocurrencies and how it can change the means of payment", and it will be addressing a little of what is the blockchain, the various cryptocurrencies that exist on the market and the roles they play and will play in our future.

Since primordial times, the need to carry out transactions has been essential for life in society, to satisfy the needs of eating, sleeping, drinking and other more secondary needs, such as buying clothes, cell phone or a computer. To suppress that needs, there is an exchange of goods and services, in which their value is defined by their seller and must be accepted by the buyer for the commercial transaction to take place. In primordial times, there was the direct exchange of goods, ten chickens for a pig, for example.

There was then the need to evolve and simplify these processes, with the insertion of bronze coins in 1000 BC in China. Subsequently, precious materials such as gold and silver were used so that the coins had a greater value.

Later, there was the introduction of the use of paper, as a replacement for currencies, which takes us to the present day, in which we make payments in various ways, whether through credit cards, through bank transfers, Paypal transfers, wearables or mobile phones. Nowadays, payments with cryptocurrencies began to become generalized, with a huge evolution in a short time, in the ways we carry out transactions and make payments. This is the result of the constant technological increase that we are witnessing nowadays, in which we need to facilitate the various daily tasks, with payments being one of the most common tasks in each person's daily life.

In fact, it appears that traditional means of payment are becoming obsolete, giving priority to payments that do not involve physical money (coins and notes), opting for the use of cards via "Near Field Communication" (NFC).). Another reason why this is happening due to the fact that we have lived through a global pandemic, in which one of the ways the virus is transmitted is through objects that have been contacted by several people, such as physical money.

An empirical analysis was conducted with the aim of verifying the possible correlation between Bitcoin, Ethereum, and the SP500 index. The main objective was to assess whether there is a potential parity between the cryptocurrencies (Bitcoin and Ethereum) and the SP500 index. The analysis included investigating their behaviors, performances, and correlations over time, attempting to identify possible patterns or significant correlations. The results showed that there is a

correlation between the cryptocurrencies due to the volatility they both share. However, no correlation was found between the cryptocurrencies and the SP500 index.

Keywords: Cryptocurrencies; Bitcoin; Blockchain; payments; Technology.

Lista de Abreviaturas e/ou Siglas

ASIC – Application-Specific Integrated Circuit

EUA – Estados Unidos da América.

IPVC – Instituto Politécnico de Viana do Castelo.

KYC – Know your costumer.

NFC - Near Field Communication.

P2P – Peer-to-Peer.

PoS – Proof of Stake.

PoW – Proof of Work.

TPS – Transações por Segundo.

Índice Geral

Índice de Figuras

Índice de tabelas

1. Introdução

O tema da dissertação, surge na sequência da publicação do "*White Paper* da *Bitcoin*" por Satoshi Nakamoto em 2008, o "criador" da rede *Bitcoin*. A sua identidade até ao dia de hoje é desconhecida, não se sabe se é um individuo, ou um grupo de pessoas, mas é considerado o "Pai" das criptomoedas. A publicação do "*White Paper* da *Bitcoin*" foi feita numa altura em que o mundo atravessava uma crise financeira, denominada de "Suprime" com enormes consequências a nível mundial, devido em grande parte ao sistema financeiro e imobiliário dos Estados Unidos que, por consequência, levou à insolvência de um dos maiores bancos de investimento americanos, o Lehman Brothers. Perante esta situação Satoshi lança um sistema que conforme ele refere, é um sistema de pagamento de *Peer to Peer (P2P)*, descentralizado[1], tendo por base a tecnologia *blockchain*. (Nakamoto, 2008).

Satoshi veio resolver um dos grandes problemas da criptografia, que até ao ano de 2008 não tinha solução, o gasto duplo[2] (Cong & He, 2018), com a implementação do sistema *Proof of Work* (*PoW*), utilizado para gerar novas moedas. Surge assim a rede *Bitcoin* e nela criada a primeira criptomoeda com o mesmo nome. A *Bitcoin* surge assim como uma moeda eletrónica sem existência física, descentralizada, que não fosse controlada por nenhuma entidade, nem bancos nem governos e que podia ser transacionada com outros utilizadores com baixos custos de transação.

Tudo isto só foi possível com a utilização da *blockchain*, uma tecnologia de dados eletrónicos descentralizada e distribuída por todos os seus utilizadores (Cong & He, 2018). Ao ser descentralizada não é controlada por uma pessoa ou entidade, mas sim por todos os seus utilizadores, que entre eles chegam a um consenso sobre a informação inserida na *blockchain*. Já as redes centralizadas são controladas normalmente por uma entidade ou pessoa, essa informação é acessível somente a quem tiver autorização. Apesar de não ser controlada por ninguém, a *blockchain* inspira confiança entre duas pessoas que não se conhecem, devido à tecnologia criptográfica[3] e às suas características. A *blockchain* conforme o nome refere é uma cadeia de blocos interligados entre si (Buterin, 2013), os blocos são armazenados cronologicamente através de um "*timestamp*"[4], estes uma vez inseridos ficam para sempre associados à *blockchain*, devido à sua imutabilidade. A tecnologia da *blockchain* consegue analisar diversa informação ao mesmo

1 Sem intermediários ou entidades externas como sistema de confiança.
2 Em Ingles "Double Spending", O double spending é o facto da informação digital poder ser copiada e, no sistema de dinheiro digital, a mesma moeda poder ser gasta mais do que uma vez. (Cong & He, 2018)
3 As características criptográficas, são utilizadas para encriptar informação, neste caso a identidade dos utilizadores, através de programação prévia, esse código só pode ser descodificado com a utilização de uma chave de desencriptação.
4 Estes "timestamps" registam o dia, mês, ano e hora que foi inserido na rede, não podendo ser alterado ou apagados da blockchain.

tempo, desde direitos de propriedade, informações fiscais, informação judicial, registos médicos, informação financeira entre outros.

Isto deve-se ao facto da *blockchain* utilizar a tecnologia de *hash*, que é o elemento que identifica os blocos, um conjunto de caracteres que torna esse bloco único[5], não permitindo haver duplicação nem alteração à *blockchain*.

Neste trabalho, será efetuada uma análise empírica que terá como amostras o índice *SP500*, a *Bitcoin* e a *Ethereum.* Irá ser analisada a cotação das três amostras, comparando as rendibilidades das suas cotações diárias e se estão relacionadas entre si, utilizando como ferramenta estatística a correlação de Pearson e de Spearman. Numa segunda fase, estudar-se-á a rendibilidade diária da cotação da *Ethereum* e se ela é afetada pela emissão de *smart contracts*. Por último, na terceira parte será analisada a variação percentual do preço médio mensal das três amostras, SP500, *Bitcoin* e *Ethereum*, averiguando se a sua variação ao longo do tempo é afetada por fatores macroeconómicos.

Por fim, esta dissertação pretende ser uma iniciação a qualquer pessoa que tenha curiosidade em saber mais sobre esta nova tecnologia que, apesar de ter quase 15 anos, ainda é muito recente e está constantemente a evoluir.

[5] O *hash* é comparado às impressões digitais, uma vez que são únicas e não é possível ser replicadas.

2. Enquadramento do tema

2.1 O que é a *blockchain*

A "temática da *blockchain*" poderá parecer complicada, e por vezes é, mas a sua conceção pode ser considerada bastante simples, uma vez que não é mais que uma base de dados de informação. Assim, para se entender melhor o que é a *blockchain*, é necessário primeiro compreender o que é uma base de dados (Cong & He, 2018).

Uma base de dados é uma ferramenta de recolha e organização de informação, onde os dados normalmente estão estruturados em formato de tabelas, o que permite serem pesquisados ou filtrados com facilidade de modo a obter-se as informações pretendidas. Uma base de dados normal caracteriza-se por ter uma entidade que controla e detém a informação armazenada, enquanto a *blockchain* é "aberta" a todos as pessoas. Esta é uma das principais diferenças entre ambas. A *blockchain* permite aos utilizadores acesso à informação que ela detém de uma forma transparente (Trautmanm, 2016), tema que irá ser abordado posteriormente.

Na *blockchain* é recolhida informação que será armazenada em blocos. Cada bloco possui um espaço limitado de armazenagem e assim que se atinge esse espaço, a informação passa para o próximo bloco em forma de cadeia, transformando-se em *blockchain* (Cong & He, 2018). A estrutura é efetuada por diversos blocos, devidamente identificados pelo seu *hash e timestamp* que estão interligados entre si. Isto faz com que a *blockchain* seja uma base de dados, mas não significa que todas as bases de dados são uma *blockchain*.

Para compreendermos a *blockchain*, é necessário perceber-se o contexto em que está implementada. Para tal, irá analisar-se a *Bitcoin*. A *Bitcoin* está implementada em vários computadores, todos ligados à *world wide web*. Não está num servidor detido por uma pessoa ou entidade, mas sim espalhada pela internet onde todos os utilizadores têm acesso a ela e podem verificar todas as transações efetuadas (Nakamoto, 2008).

A *Bitcoin* é uma *blockchain* descentralizada onde não existe uma entidade supervisora ou intermediaria, é efetuada no formato de *P2P* (Nakamoto, 2008). Isto significa que só existem duas entidades nesta rede, o comprador e o vendedor, e uma vez que não existem intermediários ocorre com baixos custos no processo conforme descrito no *white paper*[6] lançado em 2008 por Nakamoto. A tecnologia *blockchain* permite que duas partes negoceiem entre si, sem intermediários e numa troca em que não exista o problema do *double spending.* (Nakamoto, 2008).

6 O *White paper* é um documento em que apresenta os projetos da *blockchain*, o primeiro a ser apresentado foi o de Satoshi Nakamoto em 2008 quando lançou a rede *bitcoin*, são considerados os documentos fidedignos dos projetos e onde é possível verificar a tecnologia o projeto e o objetivo dessa blockchain.

2.2 Nodes

Os *nodes*, traduzindo para português os "nós"[7], podem variar dependendo do contexto em que se enquadram. Por exemplo, num sistema de rede de computadores e telecomunicações, eles oferecem propostas diferentes tendo em consideração que podem ser um ponto de redistribuição ou um terminal de telecomunicações. Podem ser físicos ou virtuais, dependendo da tecnologia em que estão a trabalhar. De forma simplificada, os *nodes* da rede são os pontos de onde uma certa mensagem pode ser transmitida recebida ou mesmo criada, sendo que serão de seguida descritos os diferentes tipos de *nodes* que existem dentro da *blockchain* (Cong & He, 2018).

A *Bitcoin* faz parte de uma *blockchain* descentralizada e que permite transações imediatas em qualquer parte do mundo, no qual não existem intermediários nestas transações e são efetuadas em P2P. A responsabilidade de interagir como um ponto de comunicação é dos diapositivos conectados à *interface* da *Bitcoin*. São considerados *nodes* porque estão a interagir entre eles e a efetuar transações dentro da rede *Bitcoin* (Nakamoto, 2008).

2.2.1 Full Nodes

Este tipo de *nodes* são os mais importantes de qualquer rede de *blockchain*, seja *Bitcoin*[8], *Ethereum*[9], *Solana*[10] entre outras. São os que dão suporte e segurança acima de tudo. Sem estes *nodes* a rede não existiria e não seria possível aceder à *blockchain*, uma vez que validam a veracidade dos blocos introduzidos na *blockchain*. Através do algoritmo de consenso da *blockchain*, verificam se o bloco é valido para integrar a *blockchain*, permitindo eles também colocar novos blocos e transações na rede.

Um *full node* tem uma cópia da *blockchain* que inclui todos os blocos e transações. Para se tornar um *full node* da *Bitcoin*, o utilizador necessita um programa, por exemplo o *Bitcoin* core, um computador com um sistema operativo Windows, Linux ou Mac, espaço livre no disco de 200 GB, 2GB memoria ram e uma conexão à internet com elevado *upload.* Além disso, tem de estar ligado todos os dias pelo menos 6 horas todos os dias imperativamente. O ideal é estar online todos os dias 24 horas, 7 dias por semana, 365 dias por ano (Vilaça Pacheco, 2021).

Atualmente, existem 9.700 *nodes* públicos ligados à rede que são voluntários ou organizações que ajudam o ecossistema. No entanto, não é possível apurar o número de *full nodes* privados porque estes operaram através de uma firewall, como por exemplo a Tor[11] estando configurados para não receber conexões (Binance, O que é Bitcoin, 2020).

[7] "Nós" na linguagem de computação são utilizados para definir a ligação entre dados.

[8] *Blockchain Bitcoin*

[9] *Blockchain Ethereum*

[10] *Blockchain Solana*

[11] https://www.torproject.org/ - A Tor é uma camada de firewall que permite navegar com mais segurança na internet, também conhecida como "cebola" devido à quantidade de camadas que tem.

2.2.2 Super *Nodes*

Os super *nodes*, também são conhecidos como os *nodes* recetíveis, estão sempre online e distribuem a informação para outros *nodes*. Basicamente, são os distribuidores de informação entre todos os *nodes*. Um super *node* confiável está ligado todos os dias à rede com várias conexões e transmitindo todas as informações e transações da *blockchain*, pelo que super *nodes* precisam de maior poder computacional do que os *full nodes*.

2.2.3 *Nodes* de mineração.

Atualmente, a *Bitcoin*, assim com a maioria das criptomoedas, é criada através da mineração computacional, ou *PoW* (Wright & Pilippi, 2015). Para isso e no caso da *Bitcoin*, é necessário adquirir ASIC (Application-Specific Integrated Circuit). Que são máquinas de mineração específicas com um custo elevado financeiramente e também a nível de consumo de energia. Estas máquinas permitem aos *nodes* juntarem-se nas designadas miner *pool*s (piscinas de mineração). Em conjunto com outros utilizadores mineraram os blocos. Um minerador solitário de *full node* usa a sua própria cópia da *blockchain*, enquanto nas *pool*s eles trabalham em conjunto, contribuindo cada um com a capacidade de mineração das suas ASIC, denominadas por *hashrate*. Numa pool só o seu administrador precisa de ser um *full node*, sendo conhecido na comunidade por *pool* miner *full node*. No final desse processo, cada *node* irá receber uma recompensa pelo seu trabalho (Peters & Panayi, 2015).

2.2.4 Clientes *lightweight* ou *simplified payment verification (SPV)*

Por fim existem os clientes *SPV*, que são os utilizadores normais das *blockchain*, que a usam sem agir como *nodes* e que, por isso, não detém uma cópia de *blockchain* nem fazem parte das verificações e validações das transações.

Basicamente, é a designação para os outros *nodes* que mesmo não participando na *blockchain*, têm acesso a certa informação da *blockchain*, podendo consultar transações incluídas num bloco, dependem sempre da informação disponível por *full nodes*.

2.2.5 Transparência da *blockchain*

A transparência da *blockchain* é um fator crucial para a confiança depositada pelos seus utilizadores, uma vez que todas as transações podem ser visualizadas pelos *nodes* ou por qualquer utilizador. Esses *nodes* têm a sua cópia privada da *blockchain* e conseguem rastrear todas as transações efetuadas (Cong & He, 2018).

Houve situações no passado em que as *exchanges* foram *hackeadas* e alguns utilizadores perderam as suas criptomoedas devido a problemas de segurança das *exchanges* ou fragilidades do código de algumas criptomoedas. Apesar da informação do *hacker* ser anónima e ser extremamente difícil ser identificado, as moedas desviadas das *exchanges* são visíveis pela comunidade, conseguindo rastrear para onde são movimentadas. O que dificultará qualquer transação que o hacker tente realizar, seja vender ou comprar bens e serviços com elas, uma vez que serão visíveis as suas transações (Hayes, 2022).

2.2.6 A *blockchain* é segura?

A *blockchain* não é totalmente segura. Existem alguns problemas de segurança, uma vez que os blocos são sempre armazenados cronologicamente estando sempre a ser adicionados ao "fim" da *blockchain*. A partir do momento em que um bloco entra na *blockchain*, é muito difícil alterar a sua informação. Para que isso aconteça terá de haver uma maioria consensual de um indivíduo ou da comunidade.

Cada bloco contém o seu próprio *hash*[12] e o *hash* do bloco anterior. O *hash code* é criado por um complexo esquema matemático que liga digitalmente números e letras. Quando alterado, altera todo o processo e consequentemente o *hash* (Peters & Panayi, 2015).

"Fazendo uma analogia simples, a segurança da *blockchain* é tão diversa como a segurança dos automóveis. Os automóveis, que se destacam pela segurança, conseguem fazê-lo porque foram criados com esse *pressuposto* e foram planeados pelos seus engenheiros por forma a serem o mais seguros possível. Não são seguros por mero acaso. Eles são testados e melhorados com o intuito de potencializar essa característica." (Vilaça Pacheco, 2021, p. 90).

A importância da segurança na *blockchain* é imperativa. Por exemplo, se um *hacker* tentar alterar a *blockchain* para roubar *Bitcoins,* adulterando a sua própria cópia, ela deixará de ser igual à dos restantes. Quando houvesse cruzamento dos dados, a do *hacker* destacar-se-ia por ser diferente das restantes e, assim, seria considerada ilegítima. Para que este ataque informático fosse bem-sucedido, o *hacker* teria de deter a maioria da *blockchain*, uma percentagem superior a 51%. Para um ataque desta magnitude seriam necessários recursos informáticos significativos para alterar todos os blocos com novos *hash*codes e *timestamps* (Hayes, 2022).

Utilizando a *blockchain* da *Bitcoin* como exemplo, o custo para realizar este ataque seria incalculável e possivelmente sem efeitos nenhuns, pois, devido à sua dimensão, quando os outros utilizadores da rede notassem tais movimentos fariam um "*fork off*", que iria originar uma nova cadeia de blocos que não estaria afetada. Isto faria com que o valor descesse, o que afetaria também o hacker, pois ficaria com um ativo sem valor nenhum (Binance, O que é Ethereum?, 2019) .

2.3 Como é utilizada a *blockchain*?

A *blockchain* funciona como armazenamento de informação sobre as transações financeiras e é considerada uma fonte fiável e segura de armazenar este tipo de informação (Nakamoto, 2008), utilizada já por algumas empresas multinacionais, como a Wallmart, Pfizer, AIG, Siemens, Unilever.

Um exemplo prático de como a *blockchain* pode ser implementa no mundo empresarial é demonstrado pela IBM nos Estados Unidos, criando o um programa, "*food trust blockchain*" (Hayes, 2022). O objetivo do programa é acompanhar todo o processo de *supply chain* desde a origem da matéria-prima ao ser recolhida e produzida, até ao momento do consumidor final (seus colaboradores). Este sistema desenvolvido e aplicado no mundo real poderia acabar com muitos

[12] No capítulo 3 será explorado detalhadamente o que é o *Hashing*.

problemas, seja a nível financeiro, ético e de saúde. A nível da saúde poderia ser implementado na indústria alimentar, uma vez que surgem muitos casos de E-coli, salmonela entre outras doenças.

Com o uso da *blockchain*, a empresa tem um controlo mais rigoroso e em tempo real da origem das matérias-primas, de todas as etapas do processo, a nível de confeção e transporte, até ao momento que é entregue aos consumidores finais. Se um ingrediente estiver contaminado, pode ser rastreado até à sua origem dando uma visão geral às empresas, permitindo às mesmas reagir com mais brevidade e possivelmente evitar que estes produtos cheguem a consumidores finais. Esta é apenas uma das muitas implementações que a *blockchain* pode ter nas nossas vidas, facilitando a mesma (Hayes, 2022).

A IBM em conjunto com a maior empresa de transporte de contentores, Maersk, implementaram uma meta de serem enviados 10 milhões de contentores em 2018 com recurso à *blockchain*, devido aos elevados custos com a documentação. Como exemplo, foi utilizado o envio de abacates do Mombasa para Roterdão, que custava 2000 € e o custo de papelada associada ficava nos 300 €, conseguindo-se com a *blockchain* reduzir o impacto financeiro, assim como o tempo da parte legal e contratual, para um valor muito inferior aos 300 €. (Allison, 2017).

2.4 Vantagens e Desvantagens da *Blockchain*

Por ser uma rede complexa a *blockchain* tem as suas vantagens e desvantagens, enumerando-se de seguida os prós e contras.

2.4.1 Vantagens da *Blockchain*:

2.4.1.1 Uma rede aberta

A *blockchain* é uma rede aberta e de fácil acesso a qualquer utilizador que pretenda fazer parte dela. Quantos mais utilizadores e mineradores tiver uma *blockchain*, mais descentralizada será. As transações da *blockchain* são aprovadas por um conjunto de computadores, diminuindo a probabilidade de erros e tornado a informação o mais transparente e fidedigna possível (Zheng, et al., 2019).

Mesmo que um computador da rede, cometa algum erro computacional, esse erro só fica agregado a essa cópia da *blockchain*. Para que esse erro se espalhasse na rede, teria de passar para 51% dos computadores. Algo que é muito complicado devido à elevada escala da *blockchain*.

2.4.1.2 Custos Reduzidos

Normalmente, em qualquer operação bancária, o reconhecimento de uma assinatura, ou mesmo a emissão de uma certidão de nascimento, é feito com recurso a um intermediário para realizar esse serviço. A *blockchain*, através da sua tecnologia eliminaria esse intermediário e com isso reduziria os custos. Numa transferência bancária, por exemplo, é necessário recorrer ao banco para ser efetuada com elevados custos e tempo de transação. Já com a *Bitcoin*, não é necessária uma entidade que realize essa transação, as taxas são reduzidas e o tempo da transferência é de minutos (Nakamoto, 2008).

2.4.1.3 Descentralização

A *blockchain* não armazena toda a sua informação num servidor ou num espaço só, mas sim copiada e distribuída por toda a internet e rede de computadores. Sempre que um novo bloco é adicionado à *blockchain*, todos os computadores ligados a essa rede são atualizados.

A informação ao ser espalhada pela internet torna-a mais difícil de ser manipulada, ao contrário da forma tradicional de estar armazenada num servidor de acesso limitado a alguns utilizares. Num cenário onde uma cópia da *blockchain* é *hackeada*, apenas essa cópia está comprometida e não toda a sua estrutura. O utilizador com a cópia corrompida pode posteriormente fazer *download* da correta (Wright & Pilippi, 2015).

2.4.1.4 Transações eficientes

As transações efetuadas num banco têm algumas restrições: não podem ser imediatas se forem de bancos diferentes, e têm custos acrescidos, pois demoram cerca de 1 ou 2 dias úteis, por exemplo. Um cheque depositado na sexta-feira à tarde só estará disponível na segunda-feira de manhã, o que impossibilita o uso desse dinheiro durante o fim de semana. Isto deve-se aos intermediários (bancos) terem um horário de funcionamento das 08:00h até as 16:00h, de segunda a sexta-feira, somente. Já a tecnologia da *blockchain*, pode resolver este problema, estando aberta 24 horas por dia, 7 dias por semana e 365 dias por ano. Tem taxas muito baixas e as transferências podem ser concluídas em minutos.

A aplicação da tecnologia da *blockchain* em transferências internacionais é algo muito útil. Uma pessoa a trabalhar em Portugal pode enviar dinheiro para outra que reside na Austrália em menos de 10 minutos. É algo extraordinário que a *blockchain* permite, sem intermediários no meio e com taxas muito baixas. A *blockchain* da Binance, por exemplo, permite realizar transferências em que as taxas são apenas de 0.01 euros (Binance, O que é Bitcoin, 2020).

2.4.1.5 Privacidade das transações

A maioria das *blockchain* operam de forma pública, o que significa que qualquer pessoa tem acesso a verificar as transações nelas efetuadas, quantos fundos foram transferidos de uma contas para outras, sem saber quem são os reais detentores dessas contas. Por isso, existe um estigma que as contas de *Bitcoin* e outras *blockchain* são anónimas (Vilaça Pacheco, 2021).

Esta informação é errónea, pois são somente confidenciais, não é fácil identificar o seu utilizador. Há *exchanges* que têm as suas contas públicas, isto porque cada utilizador tem uma chave publica e privada. Assim, quando um utilizador faz uma transação na *blockchain* que requer a sua identificação, nunca é revelada nenhuma informação privada. A segurança dos utilizadores é um fator importante (Swan, 2015).

2.4.1.6 Segurança das operações

Uma vez que a transação é colocada num bloco, a sua veracidade tem de ser efetuada por os *nodes*, colocando todo o seu poder computacional para validar essas transações. Depois de estarem validadas são adicionadas ao bloco e enviadas para a *blockchain*. Cada bloco contém o

seu *hash* único, é como uma "impressão digital" do bloco. Se por acaso alguém tentar alterar esse bloco, ele perde o seu *hash* e é colocado com outro código. O bloco seguinte já não vai conseguir fazer ligação ao bloco anterior porque o *hash* foi alterado. Este é um dos principais motivos por ser tão complicado comprometer a *blockchain* devido à sua segurança. As transações também são seguras devido a serem privadas.

2.4.1.7 Transparência

A maioria das *blockchain* são de "*open code*", isto é, qualquer pessoa pode utilizar o código das *blockchain* e adaptá-lo para as suas necessidades. Com esta transparência, qualquer pessoa pode sugerir alterações de melhoria à *blockchain*. Se houver um consenso de que a proposta dessa pessoa será para melhorar a *blockchain*, poderá ser implementada depois de uma votação (Buterin, 2013).

Um dos fatores importantes da *Bitcoin* e de outras *blockchain* é que não existem quaisquer restrições para ter uma conta, basta ter um telemóvel ou computador e acesso a internet. Estima-se que cerca de 2 mil milhões de adultos não têm acesso a uma conta bancária, o que significa que utilizam dinheiro para pagar as compras de bens e serviços. O resto do dinheiro que têm guardam em esconderijos em casa ou noutros sítios. Estes números agravam-se mais em países subdesenvolvidos, onde a economia é toda suportada por "dinheiro vivo", o que leva a uma maior probabilidade de o dinheiro ser roubado num assalto, ser perdido num incêndio ou danificado por qualquer outro acontecimento.

Se esse dinheiro estivesse guardado nas suas carteiras digitais não seria perdido e estaria sempre ao disponível. A *blockchain* também poderá servir nestes países subdesenvolvidos como forma de "controlar"[13] a população, onde dados de nascimento, vacinas e toda esta informação estaria toda guardada na conta privada destas pessoas e não seria perdida. Para além de informação medica, também os contratos poderiam ser armazenados (Cong & He, 2018).

2.4.2 Desvantagens da *blockchain*:

Como em tudo na vida há sempre dois lados da mesma moeda. A *blockchain* não foge a essa regra, em que os principais problemas são políticos e a nível de regulação. A *blockchain* é descentralizada e sem controlo, o que dificulta haver consenso na regulação (Santos, 2021). Alguns países estão a trabalhar arduamente neste tema, ainda sem solução.

2.4.2.1 Custos tecnológicos e ambientais

Uma das principais vantagens da *blockchain* é poupar dinheiro, porém a criação e desenvolvimento de uma rede *blockchain* tem um custo elevado. Por exemplo, as Asic's[14], para além da sua aquisição ser dispendiosa, consomem muita energia. A título ilustrativo, o consumo

[13] Poderá ser utilizada para ter registo médico das pessoas, e também pode ser utilizada em eleições em países do terceiro mundo.

[14] Máquinas para minerar *Bitcoin*

anual de mineração de *Bitcoin* é o mesmo da Dinamarca. Apesar destes custos elevados de eletricidade, os mineradores continuam a investir em *hardware* caro e no consumo de eletricidade, com algumas "*farms*" a utilizarem painéis solares para reduzir custos (Vilaça Pacheco, 2021).

2.4.2.2 Velocidade

A *blockchain Bitcoin*, para validar e adicionar um bloco à rede precisa de 10 minutos, uma vez que o sistema de *PoW* só consegue processar 7 transações por segundo (TPS). Por outro lado, há *blockchains* que conseguem processar 30,000 TPS. Assim, existe ainda um longo caminho a percorrer na *blockchain* para ser implementada a nível mundial. É necessário que estes números sejam superiores para que a rede seja massificada (Binance, O que é Bitcoin, 2020).

2.4.2.3 Atividade Ilegal

Este é um dos temas mais controversos e negativos da *blockchain*: o facto de ser uma rede descentralizada onde a identidade do seu utilizador é protegida, leva a que seja associada a atividades paralelas e ilegais como, por exemplo, ser utilizada para vender droga, prostituição ou terrorismo. Um *site* que operava na "*dark web*" foi o *Silk Road,* nos tempos primordiais da *Bitcoin* de 2011 até 2013. Permitia aos seus utilizadores navegar no website sem serem rastreados usando a tecnologia *Tor* permitindo comprar com *Bitcoin.*

Na balança de prós e contras, os pontos fortes das criptmoedas superam os contras. Mesmo antes das criptomoedas, os terroristas e os criminosos conseguiam movimentar o seu dinheiro através de outros esquemas, e se as criptomoedas deixarem de existir, vão surgir outras formas de lavar dinheiro (Hayes, 2022).

2.4.2.4 Regulação

A regulação é um fator importante no mundo das criptomoedas. Será preciso bastante tempo e dinheiro para ser implementado pelos governos, porque é difícil acompanhar algo que é descentralizado como a *Bitcoin*. Alguns governos baniram as criptomoedas porque não conseguiam arranjar uma solução viável para legislar. É possível comprar criptomoedas nesses países, através de empresas como a revolut e o Paypal (Santos, 2021).

2.4.2.5 Tributação

A tributação das criptomoedas é extremamente importante para aos governos, pois há impostos que não estão a ser cobrados. Os Estados Unidos da América (EUA) é um dos países onde as criptmoedas são tributadas, de forma igual a qualquer outro ativo, tendo em consideração o ganho ou perca de capital. Se for a principal fonte de rendimento como o salário ou a prestação de serviço também será sujeito a tributação.

A tributação depende de vários fatores e principalmente da localização geográfica. Por exemplo, em Portugal a taxa de mais valias é 28% sobre os ganhos financeiros, enquanto nos EUA, se for detentor de criptmoedas há menos de um ano e vendê-las, será tributado à taxa de imposto é de 37 %. Se detiver criptomoedas por um período superior a um ano, só irá ser tributado em 20%. Esta situação leva os investidores a ter uma visão a longo prazo de modo a ter um "beneficio fiscal"

de imposto e só pagar 20 % de mais valias. É importante referir que cada país tem o seu sistema fiscal (Santos, 2021).

2.5 Contratos inteligentes – (*Smarts contracts*)

A primeira vez que surgiu o conceito de contratos inteligentes (*smart contracts*) foi em 1994, apresentado por Nick Szabo (1994), em que definia os contratos inteligentes como uma ferramenta capaz de tornar as redes de computador seguras, combinando protocolos com as interfaces dos usuários, e em que explicitava onde poderiam ser utilizados: em contratos habitação, contratos direitos de autor e contratos de arrendamento (Szabo, 1994).

No mundo das criptomoedas, os contratos inteligentes são definidos como uma aplicação ou um programa a serem executados na *blockchain*, em que, por norma, são um acordo digital com um conjunto de regras previamente predefinidas através de código informático. Posteriormente, são replicados por toda a rede informática (Cong & He, 2018).

Os contratos inteligentes da *blockchain* permitem criar protocolos confiáveis que não exijam a supervisão de um terceiro, ou seja, são realizados por duas partes apenas. Quem controla estes contratos é a *blockchain* que dá a garantia que se todos os compromissos assumidos no contrato não forem garantidos, o contrato não é executado. A execução dos contratos inteligentes, através da utilização da *blockchain*, permite a redução dos custos operacionais (Vilaça Pacheco, 2021).

A *Bitcoin* foi das primeiras plataformas a dar suporte aos contratos inteligentes, mas não é graças à *Bitcoin* que eles se tornaram populares. Foi graças a Vitalik Buterin, que em 2014 criou a *Ethereum* (uma rede que será explorada mais à frente devido a ser a segunda criptomoedas mais influente no momento). A *Ethereum* é uma *blockchain* que tem contratos inteligentes e permite que outras *blockchains* sejam criadas dentro dela (Buterin, 2013).

Um contrato inteligente funciona como um programa que executa tarefas especificas com condições já pré-definidas que, estando reunidas, permite a sua execução. Esses contratos seguem regras lógicas que são previamente programadas para esses fins, como por exemplo, “se 1 + 1 = 2 então o resultado é 2” (Szabo, 1994).

O contrato tem autonomia própria, podendo automatizar todas as suas tarefas e não podem ser alterados após a sua implementação (Buterin, 2013). Os contratos são personalizáveis para as necessidades de cada pessoa ou serviço, podendo ser codificados para aplicações descentralizadas, uma vez que a *Ethereum* é uma *blockchain* que permite que outras *blockchain* sejam implementadas dentro delas.

Outro ponto importante é facto de os contratos serem transparentes, implementados em *blockchain* públicas e o seu código imutável. A confiança que os utilizadores colocam na *blockchain* deve-se ao facto da *blockchain* garantir a precisão dos seus dados, quando um contrato é executado (Zheng, et al., 2019).

Apesar dos *smart contracts* serem contratos complexos, é possível serem eliminados. Para isso, têm de incluir uma função “*selfdestruct*” no código. Existem também os contratos inteligentes

atualizáveis, que permitem aos programadores uma maior flexibilidade na imutabilidade dos contratos, com diferentes graus de complexidade. Por exemplo, um contrato inteligente pode ser dividido noutros mais pequenos, sendo alguns deles imutáveis, enquanto outros têm a função de "*selfdestruct*", permitindo esta função que sejam excluídos ou substituídos sem comprometer a funcionalidade principal. (Zheng, et al., 2019).

Os contratos inteligentes são constituídos por códigos programáveis, são personalizáveis e podem ser projetados para vários serviços e soluções. Alguns deles são descentralizados e autoexecutáveis, permitindo maior transparência e redução de custos operacionais. Existe também a possibilidade de aumentar a eficiência e reduzir despesas dependendo de cada implementação (Hayes, 2022).

Porém, existem várias limitações dos contratos inteligentes, pois ao serem criados com linguagem de programação, desenvolvida por humanos, é suscetível a erros, vulnerabilidades ou *bugs*. Assim, devem ser criados por pessoas dotadas e experientes, porque envolvem dinheiro e informação confidencial.

O facto de os contratos serem imutáveis é um fator positivo para algumas situações, mas negativo para outras como, por exemplo, no caso das organizações autónomas descentralizadas (*DAO*). A rede inicial de *Ethereum* foi *hackeada* em 2016 com milhões de *Ether* a serem desviados, devido a falhas no código do contrato inteligente *DAO*. Como o contrato inteligente era imutável, os programadores não conseguiram corrigir o problema do código, o que deu origem ao designado *hard fork*. (conceito que irá ser abordado mais à frente, neste trabalho). Foi possível "reverter" a situação e devolver os valores aos seus proprietários, criando uma nova *blockchain Ethereum*. A antiga como é imutável e não foi apagada, ficou conhecida como a *Ethereum Classic*. Este acontecimento não se deveu a uma falha da rede *Ethereum*, mas sim devido a uma implementação defeituosa de um contrato inteligente desenvolvido na rede *Ethereum* (Cong & He, 2018).

2.6 As moedas fiduciárias e as *stablecoins*

A moeda fiduciária tem um valor garantido pelo seu emissor, por norma os governos ou instituições bancarias. Portugal tem o euro, os EUA têm o dólar e o Reino Unido a libra. Estas moedas são emitidas na base da confiança (fidúcia), a população acredita que a nota de cinco euros vale cinco euros, porque o governo e o banco central europeu dão garantias que essa nota tem esse valor. Com esse pedaço de papel que vale cinco euros, é possível comprar bens e serviços, investir ou economizar (Binance, O que é Moeda Fiduciária?, 2019).

As moedas fiduciárias vieram substituir os metais preciosos, como o ouro, prata e certas *commodities*. Quando nascemos o dinheiro está presente na sociedade, por isso não questionamos a sua origem, como é gerido e quem decide o seu valor, acreditamos que ele foi criado da forma mais harmoniosa possível e que a existência do dinheiro de hoje será o mesmo de amanhã. Porém, a história tem provado o contrário, e o dinheiro varia de valor ao longo do tempo, sendo a principal causa de crises financeiras e económicas que temos atravessado (Vilaça Pacheco, 2021).

Antes das moedas fiduciárias, o ser humano trocava bens sem uma referência de valor absoluto. Um agricultor que tivesse uma boa colheita de cereais, trocava o seu excesso com um pescador que tivesse pescado mais do que precisava, depois trocavam ainda por outros bens essenciais como carne, ovos, leite e outros. Não existindo nada que quantificasse o valor dos bens, sendo apenas trocado por necessidade ou desejo (Vieira, 2017).

A origem das moedas fiduciárias remonta ao século XI (Vieira, 2017), na China. Começaram a transacionar um papel-moeda como substituto às pedras preciosas. No continente europeu apareceu somente no século XVII, utilizado maioritariamente por países como Holanda e Suécia. Porém na Suécia foi um fiasco e a monarquia sueca acabou por abandonar esse sistema, voltando a utilizar a prata como "moeda corrente".

"O ouro, pela sua raridade e características únicas entre os metais, tornou-se uma referência global em termos de valor. Em pouco tempo, os reis e imperadores começaram a cunhar as suas moedas, a maioria das vezes, com o seu rosto, sinal do seu aval perante o valor da sua moeda." (Vilaça Pacheco, 2021, p. 36).

Nos tempos modernos, durante a presidência de Nixon os Estados Unidos da América abandonaram definitivamente o padrão ouro e implementaram a moeda fiduciária alterando o estigma mundial. O sistema padrão permitia trocar notas de papel por ouro, era feito uma "livrança" em que depositavam uma quantia de ouro no banco e eles emitiam um papel com a quantidade de ouro, este servia para gastar na aquisição de bens e serviços. Com o sistema de *commodities*, os governos e bancos só emitiam essas notas se tivessem o equivalente a isso em reserva de ouro (Vilaça Pacheco, 2021). Este sistema era limitado, pois não permitia aos governos criar dinheiro e aumentar a quantidade das suas moedas. Já no sistema da moeda fiduciária, os bancos e governos tem total controlo sobre o sistema monetário e tem na sua posse diferentes ferramentas para combater crises, como utilizar as reservas, imprimir dinheiro (Luz Vieira, 2020).

Existem diferentes pensamentos referente às moedas fiduciárias e padrão ouro. Alguns referem que o padrão ouro é um sistema que funciona bem quando é baseado nas *commodities*, porque tem um suporte físico e valioso para sustentar o seu preço. Já os defensores das moedas fiduciárias afirmam que o preço do ouro não é estável, e sofre variações ao longo do tempo. Apesar de nos dois métodos os preços da moeda e das *commodities* flutuarem, os governos, nas moedas fiduciárias, têm mais flexibilidade para intervir numa situação de crise económica, como está a acontecer nos EUA, pois para combater a pandemia de Covid-19, o governo imprimiu dinheiro para distribuir pelo povo. Porém, esta solução irá trazer problemas a longo prazo (Luz Vieira, 2020).

"A quebra do banco Lehman Brothers, em setembro de 2008 – um dos grandes marcos da atual crise económica e a maior falência da história dos Estados Unidos –, ocorreu há pouco mais de cinco anos. E, até hoje, seguimos sentindo as repercussões dessa grande crise. No mainstream da ciência económica, muito ainda se debate sobre as reais causas da débacle financeira. A ganância, a desregulamentação do setor financeiro, os excessos dos bancos ou, simplesmente, o capitalismo, são todos elementos apontados como os causadores da crise. Mas é justamente o setor

financeiro, aquele em que a intervenção dos governos é mais presente e marcante, seja em países desenvolvidos, seja em países em desenvolvimento." (Ulrich, 2014, p. 35).

De seguida, irá enumerar-se alguns prós e contras da utilização de moedas fiduciárias:

2.6.1 Escassez

A moeda fiduciária não tem escassez, elas podem ser produzidas, desde que exista as matérias-primas e as máquinas para cunhar as moedas ou imprimir as notas. O facto de não haver escassez, leva muitas vezes a que os governos emitam moedas a tentar solucionar os problemas a curto prazo, descurando problemas futuros (Binance, O que é Moeda Fiduciária?, 2019).

2.6.2 Custo

O custo de produção de dinheiro em papel é relativamente elevado. Tem de se adquirir máquinas extremamente sofisticadas para cumprir com os elevados padrões de segurança e qualidade exigidos pelos governos e bancos. Por outro lado, é necessário consumir enormes quantidades de matérias-primas e os gastos de produção são elevados.

2.6.3 Globalidade

Existem várias moedas a nível mundial, algumas até implementadas em vários países, como o euro, utilizado em vários países europeus, assim como o dólar, que é a moeda mais utilizada a nível mundial.

As moedas fiduciárias são muito mais práticas em relação ao ouro, uma vez que são leves e fáceis de transportar, de proteger e de criar, ao contrário do ouro que é finito e escasso.

2.6.4 Ausência de valor intrínseco

As moedas fiduciárias não possuem valor intrínseco. Graças a isso, os governos têm maior facilidade em criar moedas, porém tal não é aconselhável, pois leva a graves problemas económicos, como está a acontecer na Venezuela neste momento. Historicamente, tem-se verificado que a implementação de sistemas da moeda fiduciária, causam colapsos financeiros (Vilaça Pacheco, 2021).

As criptomoedas poderão num futuro próximo substituir as moedas fiduciárias, pois ambas partilham certas características. No entanto, há duas grandes diferenças: enquanto as moedas fiduciárias são controladas pelos governos, as criptomoedas são descentralizadas, não têm nenhuma entidade que as controle, apenas são controladas pela *blockchain*. A outra grande diferença é a oferta, pois as moedas fiduciárias não têm qualquer limite de emissão, enquanto as criptomoedas têm uma oferta limitada, como por exemplo a *Bitcoin*, que tem um limite de 21 milhões de moedas em circulação (Nakamoto, 2008).

2.7 As *stablecoins*

As *stablecoins,* traduzindo para português "moedas estáveis", são assim designadas porque não são suscetíveis à volatilidade do mercado das criptomoedas. São ativos de baixa volatilidade, dando aos seus proprietários segurança. As *stablecoins* protegem os investidores da volatilidade, servem especialmente para transações de compra e venda de bens e serviços e estão indexadas a uma moeda corrente, como por exemplo o dólar ou o euro. Somente têm o risco da flutuação associadas a essas moedas (Redação, 2020).

Já a *Bitcoin* ou *Ethereum*, por exemplo, podem valorizar ou desvalorizar, durante um único dia, mais de 20%. As *stablecoins* não têm esta volatilidade, conferindo uma segurança extra para efetuar transações (Binance, O que é Moeda Fiduciária?, 2019).

As *stablecoins* podem ser indexadas ao ouro, petróleo ou mesmo prata, e também as moedas fiduciárias locais (euro, dólar, etc.). A China está a ponderar lançar o yuan online (Vilaça Pacheco, 2021).

Uma das *stablecoins* que integra o top 10 das criptomoedas com maior capitalização é a *Thether* (USDT), que tem o valor de 1 dólar. Apesar de não ser ainda reconhecida oficialmente pelo banco dos Estados Unidos, já é considerado o dólar digital por muitos investidores, utilizado para várias transações, seja para compra de bens ou serviços, seja para troca por outros criptoativos.

2.7.1 Quais são as principais *stablecoins*?

Existem centenas de *stablecoins* em circulação atualmente. A maioria delas estão indexadas ao dólar americano, considerado a moeda mais poderosa do mundo. A *USDT* é a principal, mas também existe a Binance USD (da *Exchange* Binance). No top 10 das *stablecoins*, nove delas estão indexadas ao dólar americano, outras ao ouro, petróleo e algumas a *commodities*. O essencial para a perseverança das *stablecoins* é o valor equivalente ao seu valor em circulação. Para mitigar este perigo de insolvência as entidades dão *reward's* para que as pessoas que tenham estas *stablecoins*, façam *stake* das mesmas.

De seguida irão ser analisadas as diversas *stablecoins* que existem no mercado atualmente:

***Stablecoins* centralizadas**: consistem no modelo de emissão de *token* indexado a uma moeda, por exemplo, o dólar ou o euro. Este é um modelo arriscado pois quem emite *os tokens* são os seus criadores e é difícil confirmar se efetivamente têm as reservas de *tokens* que estão a emitir. A moeda principal deste modelo é a mais conhecida das *stablecoins,* e já anteriormente referida*, Tether* (USDT) (Redação, 2020).

***Stablecoins* criptocolateralizadas**: são *stablecoins* que utilizam um colateral descentralizado, que pode ser a solução para o grave problema da relação de confiança face ao emissor. Estas *stablecoins* estão indexadas a criptomoedas descentralizadas como, por exemplo, o *Ether* (da rede *Ethereum*). Uma vez que estão indexados a ativos voláteis, também estão sujeitas a um pouco de volatilidade (Redação, 2020).

Stablecoins Commodities: estão indexadas a ativos como imóveis, peças de arte ou metais preciosos, por exemplo. Estas *stablecoins* variam consoante o valor dos ativos subjacentes. Apesar de terem o nome de *stablecoins,* são consideradas de risco, pois normalmente sofrem muita flutuação, uma vez que os ativos a que estão indexadas são voláteis (Redação, 2020).

***Stablecoins* não-colaterizadas**: Estas *stablecoins* não estão indexadas a nenhum ativo. O que mantem o valor desta moeda digital estável são os algoritmos que controlam a quantidade em circulação. Existe a emissão de *token* regularmente para que o preço da moeda se mantenha igual, ou o mais próximo ao rácio 1:1.

A grande popularidade das *stablecoins* devesse ao facto de tentarem oferecer o melhor de dois mundos, a segurança digital, a privacidade dos pagamentos e a velocidade de transações, reduzindo a instabilidade e volatilidade das criptomoedas (Redação, 2020).

2.7.2 A relação então as criptomoedas e as *stablecoins*.

A *Bitcoin* surgiu com o intuito de ser utilizado como dinheiro digital. O facto de ser uma moeda com elevada volatilidade não permitiu que fosse implementada como moeda corrente, mas sim como um ativo.

Já as *stablecoins* estão interligadas entre o mundo financeiro e as *blockchains*. O grande objetivo das *stablecoins* é resolver a alta volatilidade das criptomoedas, ser de livre circulação e descentralizada.

As *stablecoins* são extremamente eficientes nos pagamentos digitais, de bens ou serviços, *staking* ou transferências para todo o mundo, sem os inconvenientes da volatilidade das outras criptomoedas. Podem também ser integradas em várias aplicações devido ao seu código ser de domínio público, uma vez que estão indexadas a vários ativos reais. As taxas de transações também são muito baixas, protegendo os seus detentores em momentos de grande volatilidade do mercado das criptomoedas (Vilaça Pacheco, 2021).

2.8 Empresas que já aceitam pagamento com moedas virtuais

As criptomoedas estão a alterar o paradigma de pagamentos, pois já são aceites por algumas multinacionais líderes nos seus setores, como é a Tesla*,* Revolut *e* Amazon*.* Estas empresas estão a aproveitar esta mudança para implementar pagamentos em criptomoedas, apesar de ainda não ser algo garantido no futuro.

Algumas empresas mundiais já adotaram o pagamento dos seus serviços através de criptomoedas, dando preferência à *Bitcoin*. Os bancos mais importantes a nível mundial estão a adaptar-se a esta nova realidade, como a reserva federal dos EUA e o banco Popular da China, que estão a tentar criar o dólar digital e o yuan digital (Vilaça Pacheco, 2021).

2.8.1 Tesla

A Tesla, líder mundial no segmento de carros elétricos, aceitou temporariamente pagamentos em *Bitcoin* para aquisição de carros. Elon Musk, CEO da Tesla, foi uma das pessoas com mais

influência no mundo das criptomoedas, conseguindo influenciar o mercado com os seus *tweets*. Por exemplo a *dogecoin,* uma criptomoeda que nasceu como um *meme*, teve um aumento acima do esperado devido à atenção que o Elon Musk deu a esta criptomoeda com os seus *tweets.*

A Tesla comprou 1.5 mil milhões de dólares em *Bitcoin*, e começou a aceitar pagamentos nesta criptomoeda, originando um aumento do seu valor. Esta medida só durou 2 meses, uma vez que o próprio Musk decidiu suspender os pagamentos em *Bitcoin*, alegando questões ambientais. Quando a pegada ambiental desta moeda diminuísse, a política de aceitar *Bitcoin* seria novamente implementada, o que até aos dias de hoje não aconteceu. A Tesla vendeu metade da posição que detinha em *Bitcoin,* mas continua a deter 50% das unidades que comprou inicialmente. A SpaceX, outra empresa detida por Musk, também tem *Bitcoin* como ativo financeiro. Sendo uma empresa do ramo de exploração espacial, aceitou um pagamento em *dogecoin* para colocar um satélite na lua (Nunes, 2021).

2.8.2 Paypal e Venmo

O Paypal e a Venmo também já aceitam pagamentos em *Bitcoin*. A Paypal permite vender, comprar e deter criptomoedas, já a Venmo, empresa detida pela Paypal, que se assemelha ao conceito português de MBWay, permitiu comprar e vender algumas criptomoedas, como *Bitcoin*, *Ethereum*, *Litecoin*, e *Bitcoin* Cash. Infelizmente estas duas aplicações não permitem transferir os ativos para outras carteiras, aplicações ou *exchanges*, tendo que os utilizadores os deterem nas suas próprias aplicações (Nunes, 2021).

2.8.3 Visa e MasterCard

A Visa e Mastercard, duas empresas que dominam o mercado dos cartões bancários, estão a associar-se às criptomoedas. A Visa está associada a duas das maiores *exchanges* do mercado, a Binance e a Crypto.com que oferecem aos seus clientes um cartão de crédito onde é possível um *cashback* de 3 ou 5 % pelas compras efetuadas.

A *Visa* reconheceu, numa entrevista à CNBC, que o mercado financeiro já movimentou mais de mil milhões de dólares através desses cartões. Passou a permitir que sejam realizadas transações utilizando a *USDC coin*, uma *stablecoin* que está indexada ao dólar americano, ou seja, acompanha sempre o valor do dólar (Nunes, 2021).

Por sua vez, a Mastercard anunciou em abril uma parceria com a corretora de criptomoedas Gemini, através da criação de um cartão de crédito que permitirá aos seus utilizadores realizar compras com mais de 30 criptomoedas e obter um *cashback* de 3%.

2.8.4 Revolut

A Revolut é um dos principais impulsionadores da mudança nos meios bancários, sendo um dos primeiros neobancos (banco completamente online). Desde o fim de 2017, permite comprar e vender criptomoedas, embora não possua uma grande variedade de ofertas. Outro fator negativo deste serviço é os utilizadores deste banco não serem os detentores legais deste ativo, a custodia pertence ao banco. Além disso, existem elevadas taxas para transacionar os criptoativos.

2.8.5 Goldman Sachs, Morgan Stanley e JPMorgan

A banca norte-americana aderiu às criptomoedas a partir do "boom de 2017", mas de forma indireta através de instrumentos derivados.

O banco Morgan Stanley criou um departamento da gestão de património, permitindo aos seus clientes transacionar três fundos de investimentos que dão exposição às potenciais subidas e descidas da *Bitcoin*.

Já o JPMorgan, permitiu desde 2021 que os seus clientes negoceiem títulos de um fundo de investimento em criptomoedas utilizando o Graysacle *Bitcoin Trust*. Fornece também outros serviços para a *Ethereum*, *Bitcoin Cash* e *Ethereum* Classic

2.9 O que é o *Hashing*?

O *hashing* é o processo de geração de uma saída (*output)* de tamanho fixo a partir de uma entrada (*input)* de tamanho variável, e é efetuado através de fórmulas matemáticas. Nem todas as funções *hash* usam criptografia. O *hash* criptográfico é fundamental para manter a segurança e a funcionalidade da *blockchain*. Os níveis elevados de segurança e integridade dos dados são possíveis com a utilização da tecnologia *hash*. A função *hash* é determinística, o que significa que enquanto a entrada for a mesma, a saída também será a mesma (Binance, O que é Hashing?, 2019).

Por norma os algoritmos *hash* das criptomoedas são desenhados para serem utilizados como funções de sentido único, projetados para que um *input* dê origem a um *output.* O inverso é extremamente difícil e exige um enorme recurso computacional e temporal para se conseguir gerar um *output* através de um *input*. Quanto mais difícil for encontrar o *input*, mais seguro e confiável será esse *hash* (Binance, O que é Hashing?, 2019).

2.9.1 Como é executada uma função *hash*?

Existem diversas funções *hash* que irão gerar diferentes outputs dependendo dos seus *input*s. O algoritmo SHA-256 irá produzir *outputs* de 256bit, já o SHA-1 originará sempre um algoritmo de 160 bits.

De seguida será dado um exemplo de como o *hash* SHA-256 funciona com *input*s semelhantes, utilizando as palavras "*Bitcoin*" e "*Bitcoin*".

SHA-256	
Input	Output (256 bits)
Bitcoin	78434ec2e8ffe402144dc631b055f711225191f1624fcc63b615ac0e95daf9ab
bitcoin	b259bba3571455ca539dcd1ac9577f5e8b5da0c3662478abc1ec5833319ddca

Figura 1- *SHA 256.*
Fonte*:* Elaboraçao própria.

Com apenas a alteração da primeira letra maiúscula, gerará dois *outputs* totalmente diferentes e distintos entre eles. O *hash* SHA-256 terá sempre um tamanho fixo de 256 bit e 64 caracteres, independente do tamanho do *input*, seja ele de uma letra, ou de vinte. Utilizando sempre o mesmo *input* gerará sempre o mesmo output.

Já o *hash* SHA-1 ao ser executado através dos mesmos *input*s anteriores terá os seguintes resultados:

SHA-1	
Input	Output (160 bits)
Biticoin	17f0dc9146570c608ac9d6e0d11f8d409a1ee6ed
Bitcoin	5c14a76ff9867933c4e0893622cca0eae7be5860

Figura 2 - *SHA* – 1.
Fonte: Elaboraçao própria.

O acrônimo SHA significa *Secure Hash Algorithms* (Algoritmos de *Hash* Seguros) e representa o conjunto de funções *hash* criptográficos. O SHA-256 faz parte dos grupos de SHA-2 e SHA-3, que atualmente são considerados os mais seguros em termos criptográficos. A função *hash* tem aplicabilidades ilimitadas e é utilizada em bancos de dados, gestão de dados, criptografia entre outras áreas.

A função *hash* de criptografia é utilizada para segurança, por exemplo, na autenticação de mensagens, impressões digitais, criação de códigos, e é um dos processos mais importante de mineração e na geração de novos endereços e chaves de rede (Nabil, 2019).

Esta tecnologia aplicada à *blockchain* permite realizar várias transações simultaneamente e apoiar o processo de mineração, bem como qualquer protocolo da *blockchain.* Cada bloco lançado na *blockchain* é associado a um *hash* único, o qual é o equivalente à impressão digital do ser

humano. É altamente improvável haver duas impressões digitais (ou *hashes*) sejam idênticas, o que garante a segurança e integridade dos dados da *blockchain* (Binance, O que é Hashing?, 2019).

Corromper uma função hash é conhecido como "ataques de força bruta" (brute-force attacks). Para corromper um hash, é necessário descobrir o input utilizado. No entanto, existem milhões de possíveis *inputs* e uma simples mudança, como uma letra maiúscula, pode resultar em um *output* completamente diferente. Existe a possibilidade de diferentes *inputs* produzirem o mesmo *output*, o que é conhecido como colisão. Para que uma função *hash* seja considerado válido, ele deve atender a três critério (Nabil, 2019):

- Resistência à colisão: deverá ser inviável que dois *input*s diferentes, produzem um *hash* com o mesmo *output*. Esse é o primeiro e mais importante critério para que o *hash* seja considerado válido;
- Resistência à pré-imagem: Esse conceito previne que seja possível descobrir o *input* através de *output*, isto tem uma probabilidade muito baixa de ser encontrado. Também conhecido como *reverse engineering*, o processo de começar do final para encontrar o início e como se produz;
- Resistência à segunda pré-imagem: isto ocorre quando alguém é capaz de encontrar um *input* que tem um *output* igual a outro *input* já existente, aqui encontramos uma colisão.

Ao cumprir estes três requisitos cumpridos, pode obter-se um *hash* válido e resistente à colisão. No entanto, não garante que um *hash* nunca irá encontrar uma colisão, pois os *input*s são infinitos e os *outputs* são finitos. É importante salientar que os grupos SHA-0 e SHA-1 não são considerados seguros, enquanto o SHA-2 e SHA-3 são considerados seguros e resistentes à colisão (Binance, O que é Hashing?, 2019).

2.10 O que é a *Bitcoin*

A *Bitcoin* é a primeira *blockchain* a dar origem a uma moeda digital, anunciada pela primeira vez em 2008, através de um artigo publicado por uma pessoa ou um grupo de pessoas identificadas pelo pseudónimo “Satoshi Nakamoto”. A sua criação coincidiu com a crise financeira global de 2008 e foi presentada como uma alternativa ao sistema financeiro tradicional centralizado, que muitas pessoas consideravam ter sido o responsável pela crise que se vivia na altura.

Ao contrário das moedas fiduciárias, a *Bitcoin* não é emitida ou controlado por um banco central, mas sim um sistema de diversos computadores espalhados por todo o mundo descentralizados. Permite acesso ao utilizador à rede, através de um computador com internet. A *blockchain Bitcoin* permite enviar e receber a moeda *Bitcoin*, também conhecida por *BT*. (Nakamoto, 2008).

Os fatores que tornam a *Bitcoin* um dos ativos mais valiosos do mundo é o facto de ser descentralizada, não ter nenhuma instituição que a controla e que coloque restrições ao seu uso, ser resistente à censura e permitir que qualquer pessoa com acesso à internet possa utilizar em

qualquer parte do mundo, uma vez que não há barreiras físicas à internet (Binance, O que é Bitcoin, 2020).

Sendo um dos métodos de pagamento mais seguros do mundo, a *Bitcoin* é atualmente utilizada para pagamentos internacionais. Devido à sua criptografia, permite transferir fundos de forma anónima em todo o mundo, sem revelar a identidade dos utilizadores. Por outro lado, muitos utilizadores utilizam a *Bitcoin* como investimento a longo prazo, o que é denominado na comunidade das criptomoedas como "*HODLing*" (Vilaça Pacheco, 2021).

A *Bitcoin* é frequentemente associada ao ouro digital, por ter um valor finito disponível no mercado. Após a conclusão do último bloco de mineração, apenas 21.000.000 de moedas estarão em circulação. Com o passar dos anos, os denominados "*HODLers*" preveem que o seu valor irá aumentar significativamente, algo que tem ocorrido desde a sua criação (Binance, O que é Bitcoin, 2020).

2.10.1 História da *Bitcoin*

Até ao dia de hoje, não foi possível determinar a identidade real do criador da *Bitcoin*, introduzida em 2008 através do *white paper* por Satoshi Nakamoto, um pseudónimo utilizado para ocultar a sua verdadeira identidade, poderá ser uma pessoa japonesa, um grupo de pessoas em África ou até um governo. A sua verdadeira identidade é um dos mistérios mais importantes do mundo das criptomoedas, ao qual até ao dia de hoje não foi desmitificado. Satoshi apresentou em 2008 o projeto *Bitcoin* e até 2010, ano em que desapareceu de vez da internet, foi um assíduo utilizador do fórum onde as pessoas postavam e idealizavam o futuro do que poderia ser a *Bitcoin* e como poderia revolucionar não só o sistema financeiro, mas também o mundo (Binance, O que é Bitcoin, 2020).

A *bitcoin* é uma junção de diversas tecnologias, assenta na base da *blockchain*, a *blockchain* conforme mencionado na dissertação foi introduzida inicialmente no início dos anos 90 do século passado por Stuart Haber e Scoot Stornetta, ambos propunham um sistema de "*timestamping*" dos documentos, que impediam que os documentos fossem adulterados e protegiam a integridade e veracidade dos mesmos (Szabo, 1994).

2.10.2 Dinheiro digital antes da *Bitcoin*

Antes da *bitcoin* existir, houve diversas tentativas de digitalizar o dinheiro, para tornar mais conveniente movimentar pelo mundo. Os projetos propostos falharam na tentativa de conseguir esta façanha. A *Bitcoin* é, de longe o projeto com mais sucesso (Binance, O que é Bitcoin, 2020).

O primeiro projeto é a *Digicash*, fundado pelo criptografo e programador David Chaum, porém, devido às limitações tecnológicas dos anos 80 e a pouca utilização da internet como meio de pagamentos e a escassez do e-commerce levaram à falência da empresa.

A B-Money, é citada no *white paper* da *Bitcoin*, fundada pelo engenheiro de computação Wei Dai nos anos 90, usava um sistema idêntico ao da *Bitcoin* de *PoW*, onde os seus usuários

também seriam os que validariam as transações através de *PoW.* A *B-money* não avançou como projeto, sendo que a *Bitcoin* detém certos aspetos deste projeto.

Bit Gold, é também um dos projetos nos quais a *Bitcoin* se baseou. Existem várias teorias de que o seu criador, Nick Szabo é Satoshi Nakamoto, devido às semelhanças que existem entre ambas. No entretanto, a *Bit Gold* foi outro projeto que não avançou.

2.10.3 Como são criadas *Bitcoins*?

A *bitcoin* tem um fornecimento de moedas finito. No ano de 2020, mais de 90% do seu fornecimento já havia sido minerado. A criação desta moeda é realizada através do sistema *PoW*, que utiliza máquinas sofisticadas (*ASIC*) cujo propósito é a obtenção de moedas digitais. São máquinas extremamente potentes que consumem muita energia e possuem um elevado custo de aquisição

Para que as 21.000.000 de moedas sejam alcançadas, analistas preveem que ainda faltam 100 anos para minerar os restantes 10%. Isso ocorre devido a um processo conhecido como "*halving"*, que consiste em aumentar a dificuldade de resolver equações matemáticas (Binance, O que é Bitcoin, 2020).

A mineração da *bitcoin* é efetuada atualmente por *ASIC*, inicialmente era efetuada com processadores de computadores nos primórdios da introdução desta tecnologia (2009). Com o aumento da dificuldade (*halving),* foi necessário criar máquinas com mais capacidade computacional para decifrar os complicados esquemas informáticos.

Ao minerar os blocos, os utilizadores adicionavam os novos blocos à *blockchain*. Se o bloco for válido e aceite pela *blockchain,* esses mineradores receberão uma recompensa como incentivo pelo tempo despendido. Gerar um bloco é um processo demorado e com custos elevados tanto em termos de material como de energia (Buterin, 2013).

2.10.4 Como comprar *Bitcoin* e outras criptmoedas

Para comprar *Bitcoin*s é necessário ter uma conta criada numa *exchange*. As mais conhecidas a nível mundial são a Binance[15], Coinbase[16] e Crypto.com[17]

Para este processo, é preciso registar-se nas plataformas de *Exchange* e preencher dados pessoais, como nome, morada, associar uma conta bancária e um documento de identificação pessoal, por exemplo o cartão de cidadão ou carta de condução. Estas plataformas atualmente tem um *KYC*[18] muito eficaz, para evitar que utilizadores utilizem estas plataformas e as criptomoedas

[15] https://www.binance.com/en

16 https://www.coinbase.com/pt-PT/

17 https://crypto.com/

18 know your costumer.

para realizarem lavagem de dinheiro ou para praticarem crimes. Se uma pessoa estiver na lista de terrorismo, essas plataformas podem ser culpadas e multadas ao permitirem que criminosos criem uma conta e transacionem na sua plataforma.

Por isso o *KYC* está cada vez mais evoluído e presente nessas plataformas. Depois de a conta estar devidamente validada e ativa, é preciso aceder à aplicação mobile, ou ao site e carregar a conta, seja através de um cartão de débito ou crédito, transferência bancária ou PayPal[19]. Finalmente é só comprar a moeda *bitcoin* que será adicionada à sua conta pessoal e que poderá ser transacionada em qualquer plataforma que as aceite (Binance, O que é Bitcoin, 2020).

2.10.5 E se perder as *Bitcoins*?

Como não existe uma entidade reguladora das criptomoedas, cada utilizador é responsável pela segurança das suas próprias moedas. Se ocorrer algum problema devido a uma má utilização, é extremamente difícil reverter a transação. Por esse motivo, a maioria dos utilizadores guarda as suas moedas digitais nas *exchanges*, onde a custodia é garantida na conta de utilizador. Na *exchange,* as moedas não são detidas pelos utilizadores, mas sim pelas próprias *exchanges*. Normalmente os utilizadores que utilizam as *exchanges* é numa ótica de *trader*, para vender e comprar criptoativos regularmente. No entanto, se os utilizadores comprarem os ativos digitais como a *bitcoin* numa ótica de "*HODL*"[20] o mais comum é guardá-los em carteiras físicas (Binance, O que é Bitcoin, 2020).

Estas carteiras são o oposto das *exchanges*. O verdadeiro detentor da moeda são os utilizadores e os fundos são armazenados em carteiras digitais. Porém as carteiras não possuem de forma diretas as moedas. Ela tem uma palavra-chave que desbloqueiam as moedas na *blockchain*. Existem duas chaves: a chave publica e a chave privada. A chave publica é um endereço alfanumérico que identifica os utilizadores na *blockchain* e para o qual podem ser enviadas as criptomoedas. Este endereço pode ser compartilhado com qualquer utilizador. Já a chave privada é composta por 12 palavras *(seed-phrase*) aleatórias. Ela não deve ser guardada em diapositivos eletrónicos, mas sim num papel. Os aparelhos eletrónicos são suscetíveis a ataques informático, e o utilizador pode perder o conteúdo da sua carteira (Vilaça Pacheco, 2021).

Para guardarmos as criptomoedas existem formas distintas, as "Hot wallets"[21] e "cold wallets"[22], as carteiras de Software e as carteiras de Web (Binance, O que é uma carteira de criptmoedas, 2019).

[19] Rede de pagamento e transferências bancárias, https://www.paypal.com/pt/home

[20] "*Hodl*" é o termo utlizado nas criptomoedas para um investimento a longo prazo.

[21] "*Hot Wallets"* traduzindo para português são as carteiras quentes.

[22] "*Cold Wallets"* traduzindo par português são as carteiras frias.

A *hot wallet* é uma carteira digital que está conectada à internet, normalmente através de uma aplicação no telemóvel, ou através do computador. Por estarem sempre ligadas à rede elas são muito convenientes para realizar pagamentos, comprar e vender criptomoedas. Também são mais suscetíveis a ataques informáticos, umas das mais conhecidas é a *Trustwallet*[23], criada pela Binance a maior *exchange* do mundo (Binance, O que é uma carteira de criptomoedas, 2019).

As *Cold wallets* são carteiras que podemos considerar "*offline*" ou seja, não estão conectadas à internet, estas são muito mais seguras porque não estão constantemente ligadas à internet. Só quando for necessário movimentar os ativos é que estas carteiras são utilizadas, normalmente são *pen driver USB* (Binance, O que é uma carteira de criptmoedas, 2019).

As carteiras Web permitem o acesso à *blockchain* através do navegador do computador, seja ele o Google Chorme, Safari ou Firefox. Este é um dos métodos mais populares, pois permite aceder às criptomoedas em qualquer parte do mundo. Apesar de ser muito conveniente, para os utilizadores menos experimente pode ser um risco acrescido. Os mais comuns são o *Metamask*[24] e o *StormGain*[25] (Binance, O que é uma carteira de criptmoedas, 2019).

As carteiras de *desktop* são um *soft*ware que se instala diretamente no computador. Ao contrário das versões *web*, elas oferecem aos seus utilizadores controlo total das suas chaves e fundos. Isso significa que as chaves privadas e os endereços de acesso à *blockchain* são armazenados em um arquivo, que deve ser protegido por uma senha pessoal criptográfica. É necessário realizar um backup deste arquivo, chamado "*wallet.dat*", em um local seguro. É possível exportar a *seed-phrase* caso o computador onde o arquivo ficar danificado ou inacessível. É uma carteira segura, desde que seja utilizada corretamente e que o computador esteja livre de vírus e malwares (Binance, O que é uma carteira de criptmoedas, 2019).

As carteiras de *Hard*ware são consideradas as mais seguras, porque são instaladas em um dispositivo que não está conectado à internet, gerando vários números aleatórios para criar chaves publicas e privadas, tornando muito difícil comprometer o sistema. Apesar disso, terão de ser bem configuradas inicialmente, caso contrário, poderão comprometer a segurança. São utilizadas por pessoas que detém uma quantidade significativa de criptmoedas e pelos *HODLers*. Ao ser uma *cold wallet,* não será transacionada num curto espaço de tempo. A segurança é efetuada com a *seed-phrase* e um pin para proteger o computador (Binance, O que é uma carteira de criptomoedas, 2019).

Como o sistema é descentralizado, não existe ninguém que assegure a moeda. Por exemplo, no euro, o Banco Central Europeu é responsável pela moeda, assim como os governos. Na *Bitcoin*, cada utilizador é responsável pelas moedas e pela forma como as guarda. A responsabilidade também recai sobre as transações efetuadas. Se, por acaso, enviar as *bitcoins* para outro endereço que não seja o seu, perderá as moedas, uma vez que não é possível fazer

[23] https://trustwallet.com/pt_BR/

[24] https://metamask.io/

[25] https://stormgain.com/

alterações à *blockchain*. Para isso, teria de ter controle de 51% da mesma, o que é extremamente difícil.

Uma das formas de ganhar dinheiro com a *bitcoin* é através de *trading*, os utilizadores compram e vendem regularmente nas exchanges com o intuito da valorização da moeda. A outra forma é a de *HODLing*, em que os utilizadores compram *bitcoin* e guardam por longos períodos na esperança da sua valorização. Outra forma é através de empréstimo, nos quais serão pagos juros sobre o valor emprestado, e por último efetuando Staking também serão recebidos juros com uma taxa previamente definida (Binance, O que é uma carteira de criptmoedas, 2019).

2.10.6 O *Halving de Bitcoin*

O *Halving da* rede *Bitcoin* é um procedimento que reduz as recompensas por bloco, e esse procedimento não afeta as taxas de transação na rede. No início da *Bitcoin*, os mineradores recebiam uma recompensa de 50 *Bitcoin* por cada bloco minerado o que em 2022 seria equivalente a cerca de 2.000.000 milhões de Euros por bloco minerado. O primeiro *halving da Bitcoin* ocorreu em 28 de novembro de 2012, o valor recebido por cada bloco minerado reduziu para metade (25 BTC). O segundo foi efetuado no dia 09 de julho de 2016 reduzindo para metade novamente (12.5 BTC). O último *halving* ocorreu em maio de 2020 reduziu o valor para 6.25 BTC. Existe um padrão no código da *Bitcoin* que prevê um halving a cada 210.000 blocos minerados, o que ocorre aproximadamente a cada quatro ano (Nakamoto, 2008).

Convém realçar que a limitação do fornecimento da moeda *Bitcoin* é considerada uma das principais características da moeda. É vista como uma vantagem em relação às moedas fiduciárias, que podem ser inflacionadas através da impressão de dinheiro. Além disso, a escassez da *Bitcoin* também contribui para a sua valorização a longo prazo, sendo a oferta limitada a 21.000.000 moedas, o que pode levar a uma maior procura por parte de investidores. É importante referir que a cotação da *Bitcoin* é altamente volátil e poder sofrer enormes flutuações (Binance, O que é Bitcoin, 2020).

2.10.7 Escalabilidade da *Bitcoin*

A escalabilidade da *Bitcoin* é natural, o sistema está constantemente a evoluir e crescer. Se um utilizador tem um *website*, e quer que o *website* suporte mais tráfego e mais conteúdo, pode adicionar mais servidores para aumentar a sua capacidade. Assim como qualquer tecnologia, quanto mais potente for o *Hardware*, melhor desempenho terá esse equipamento. No contexto da *blockchain*, o termo escalabilidade é utilizado para descrever a facilidade com que a *blockchain* pode ser atualizada para processar um maior número de transações do que é capaz de processar atualmente (Binance, O que é Bitcoin, 2020).

À medida que os números de utilizadores em uma rede *blockchain* aumentam, a rede deve ser capaz de suportar esse crescimento. A *Bitcoin* funciona com pagamentos e depende da rapidez de transações. Como resultado, a *blockchain Bitcoin* precisa de escalar. Existe um limite de

transações que podem ser efetuadas por bloco e os mineradores recebem taxas de transações pela validação desse bloco (Binance, O que é Bitcoin, 2020).

A *lightning network* foi desenvolvida como uma solução para a escalabilidade da rede, consistindo em uma segunda camada na *bitcoin* (*layer two*) em vez de ser tratada pela *blockchain* normal, é submetida a outro protocolo. Ela foi criada para resolver o problema de transações da *bitcoin* em que só era possível realizar 6 a 8 transações por segundo. Com a *lightning network* os utilizadores podem enviar fundos instantaneamente (Vilaça Pacheco, 2021). Para que isso seja possível, os dois utilizadores que desejam realizar a transação bloqueiam as moedas num endereço desenvolvido só para essa transação. Esse endereço tem um protocolo especial onde executa a transferência a partir do momento que os dois participantes concordam com os termos pré-estabelecidos. Uma vez concluída a transação, as partes envolvidas mantêm um registo privado (Ulrich, 2014).

2.11 Hard and soft fork

Assim como qualquer programa informático, a *blockchain* precisa de constantes atualizações para continuar a evoluir, tornar-se mais eficiente e resolver os seus problemas. Nos telemóveis as atualizações assim como nos computadores são quase automáticas e estão pré-definidas para serem realizadas sozinhas. Se não forem atualizadas, as funcionalidades mais recentes não ficam disponíveis para os utilizadores. Nas criptomoedas, dado que o código é aberto, é mais complicado do que uma simples atualização de computador. Para ultrapassar esta barreira existem dois mecanismos, *hard fork* e *soft fork*s, que serão abordados de seguida (Vilaça Pacheco, 2021).

Para que um *fork* seja efetuado, é necessária a concordância dos três intervenientes da *blockchain*: os programadores, mineradores e os *full nodes*. Estes são os intervenientes que mais contribuem para a rede. Os programadores criam e atualizam constantemente o código da *blockchain*, que é aberto e permite aos programadores realizar alterações (Peters & Panayi, 2015). Essas alterações têm de ser validadas por outros programadores. Os mineradores são responsáveis por proteger e executar o código na rede. Eles trabalham para adicionar novos blocos à *blockchain* através do método *PoW* e são recompensados por minerar os blocos. Por fim, os *Full Nodes* são o centro da rede. Eles são os responsáveis por receber, validar e enviar os blocos e transações, mantendo sempre uma cópia da *blockchain* (Binance, O que é Bitcoin, 2020).

Um *hard fork* é uma "copia" efetuada da *blockchain*, ou seja, a *blockchain* original contínua a existir e nasce outra. Por exemplo, vamos imaginar que 50 % da *blockchain* quer seguir um rumo e o outro 50% quer seguir outro rumo. É criado um *fork* em que ambas as *blockchain* vão existir. É como se uma estrada inicial com um só rumo, a qualquer momento se dividisse em duas. Isso não significa que elas deixem de ter a estrada em comum, mas sim que teve de se dividir para dar origem a duas estradas secundárias. Uma vez que a maioria dos projetos é código aberto, isto acontece regularmente. No entanto existe uma distinção entre *hard fork*s e *soft fork*s (Binance, O que é Bitcoin, 2020).

Um *hard fork* é uma atualização de *soft*ware em que é incompatível com as versões anteriores de *blockchain*. Eles ocorrem quando os *nodes* adicionam regras novas que entram em conflito com as regras antigas. Como resultado deste conflito, são criadas duas *blockchain*s distintas, uma com as regras antigas e outra com as regras novas. A partir dessa criação, duas redes funcionam em paralelo e novos blocos são gerados em cada uma das *blockchains*. Elas não estão mais interligadas e os *nodes* de ambas partilham a mesma *blockchain* até ao momento do *fork*, a partir dai os blocos e as transações são separadas (Binance, O que é Bitcoin, 2020).

Em 2017, ocorreu um *hard fork* na rede *Bitcoin*, houve consenso que se deveria dividir a *blockchain* porque queriam aumentar o tamanho dos blocos. Os *nodes* originais não queria alterar porque o aumento de tamanho, seria contra o código original. Após vários debates foi criada a *bitcoin cash* (*BCH*) (Vilaça Pacheco, 2021).

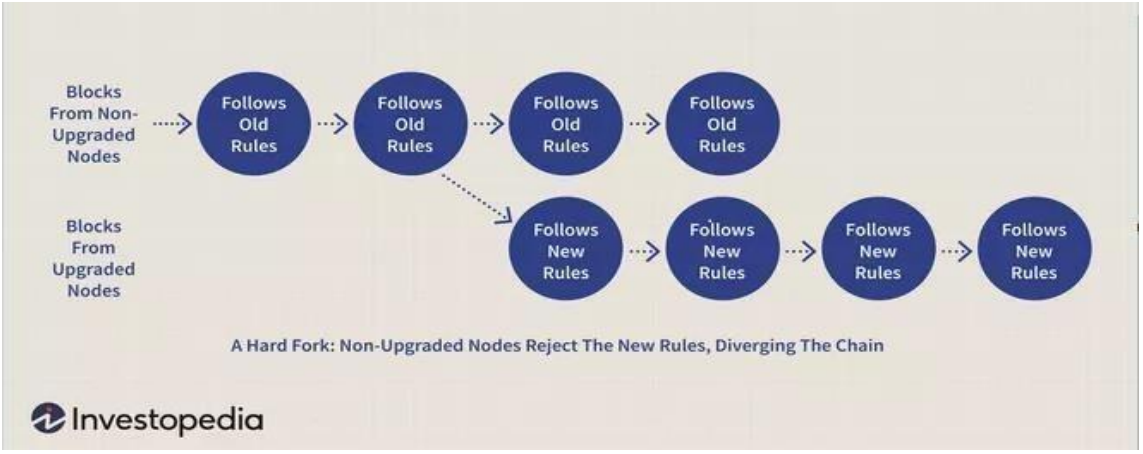

Figura 3 - *Hard fork.*
Fonte: Julie Bang, Investopedia 2019.

O *Soft Fork* é uma atualização menos disruptiva na rede, que continua a ser compatível com as versões anteriores da *blockchain*. Qualquer adição de novas regras, como não altera a *blockchain* é aceite pelos *nodes*. Por exemplo, a diminuição do tamanho de um bloco não afeta a *blockchain*, enquanto o aumento do tamanho do bloco afetaria. Se os *nodes* optarem por não atualizar para o *soft fork*, eles ainda podem comunicar com outros *nodes*, mas podem filtrar certas informações que são enviadas (Binance, O que é Bitcoin, 2020).

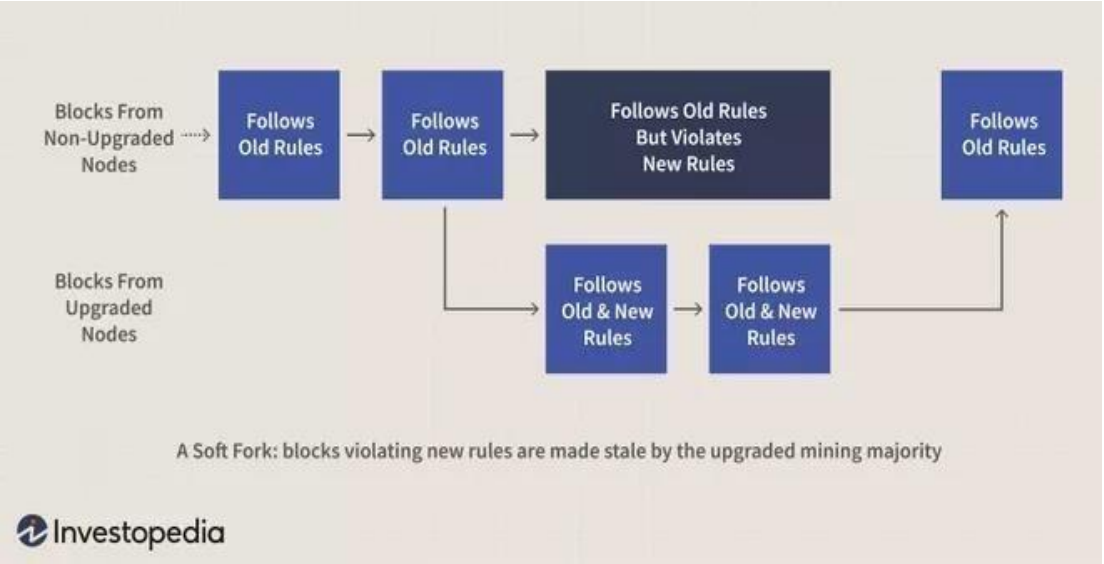

Figura 4 - *Soft fork.*
Fonte: Sabrina Jiang, Investopedia 2020.

2.12 Ethereum

A proposta inicial da *Ethereum* foi desenvolvida pelo seu co-fundador, Vitalik Buterin, que publicou a ideia num blog em 2013. A proposta consistia numa blockchain descentralizada capaz de executar qualquer aplicação e que poderia evoluir constantemente, com os limites impostos somente pela criatividade dos seus programadores. O objetivo da *Ethereum* era explorar o potencial da *blockchain* para além do projeto inicial da *Bitcoin*. A *Ethereum* é atualmente uma das principais *blockchains* e a segunda criptomoeda mais valiosa, permitindo o desenvolvimento de outras *blockchains* e *softwares* dentro da sua rede descentralizada. Além disso, a *Ethereum* também é utilizada como meio de pagamento para trabalhos realizados dentro da blockchain, com a sua moeda sendo chamada de "*Ether"* (Buterin, 2013).

A *Ethereum* foi criada em 2014 por Vitalik Buterin e Joe Lubin, que publicaram o *white paper* no mesmo ano. Em 2015, foi realizada uma campanha de financiamento (*crowdfunding*) com enorme sucesso. A campanha de financiamento da *Ethereum* foi uma das mais bem-sucedidas de sempre. Foram fornecidos 72 milhões de *Ether*, sendo que 50 milhões desses *tokens* foram disponibilizados na venda pública, conhecida como *Initial Coin Offering (ICO*). A *ICO* é a disposição de *token* no mercado, para quem quiser comprar a troco de dinheiro ou outra criptomoedas (Swan, 2015).

A *blockchain Ethereum* é um sistema *open source*, seguro, descentralizado e com escalabilidade, o que a torna a principal escolha dos programadores para criar outras *blockchains* ou *tokens*. A tecnologia *ERC-20* é a ferramenta essencial para a criação de criptomoedas e aplicações descentralizadas na plataforma *Ethereum*. Com *ERC-20*, os programadores podem criar tokens personalizados na rede *Ethereum* com características específicas. Isso possibilita a criação de uma grande variedade de *tokens*, cada um com suas próprias funcionalidades e casos de uso (Vilaça Pacheco, 2021).

Devido a estas características é considerada a "mãe" das *blockchain* atuais. Permitindo que outras sejam criadas dentro dela. Uma analogia bastante simples seria considerar a *Ethereum* como o sistema operativo do computador (Windows) e as restantes *blockchains* e criptomoedas as aplicações (Binance, O que é Ethereum?, 2019)

2.12.1 O que alimenta a rede *Ethereum*?

O *Ethereum* gás é o combustível da rede, necessário para o poder computacional executar os milhares dos *smarts contracts* na *blockchain*. Este conceito foi criado para prevenir que um *smart contract* seja configurado para ser executado indefinidamente, o que sobrecarregaria o sistema e levaria a *blockchain* colapsar (Binance, O que é Ethereum?, 2019).

Houve então criação do *gwei* (a unidade de medida da rede *Ethereum)* que funciona como uma taxa para a execução dos *smart contract*. Isso mitigou o risco do *smart contract* ser executado indefinidamente. Assim como um carro precisa de combustível para se deslocar, o *smart contract* também necessita do combustível (gás) para ser executado. Existe uma quantidade de *gwei* previamente definida para esse contrato ser executado, de forma a não gastar mais do que o necessário. Se não houver gás suficiente, o contrato não é executado. O gás é, portanto, um mecanismo de taxa, em que os contratos mais complexos consomem muito mais gás que os mais simples (Buterin, 2013)

O preço do *gwei* varia bastante e é estabelecido pelos mineradores. Ao realizar uma transação na rede, se houver congestionamentos e muitas transações o preço será mais elevado. Já o oposto também acontece, quantas menos transações forem efetuadas mais barato será o *gwei* (Binance, O que é Ethereum?, 2019).

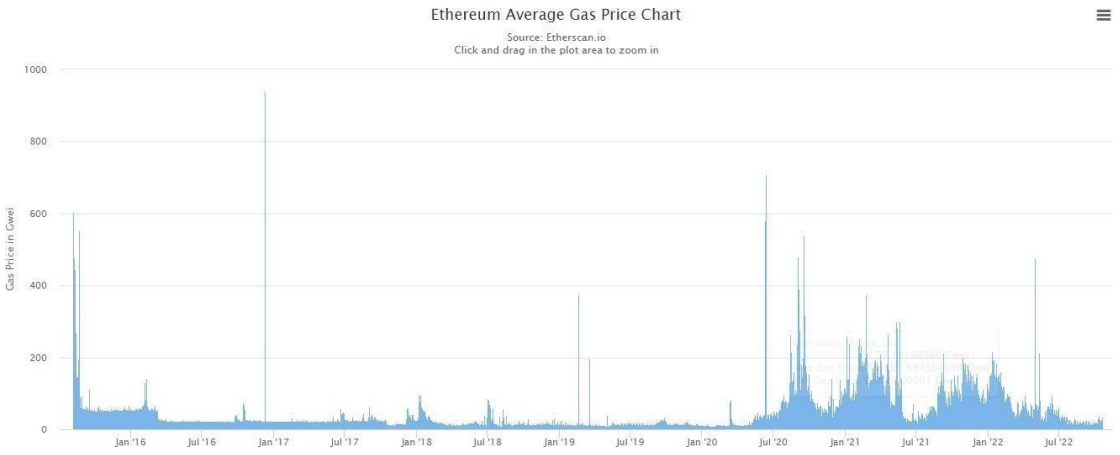

Figura 5 - Preço médio de *gwei.*
Fonte*: Etherscan.io*

Para realizar uma transação de um *smart contract*, primeiro é necessário definir o montante de *gwei* que esse contrato necessitará. Para ter prioridade sobre os outros poderá ser pago um preço de *gwei* superior para incentivar os mineradores a darem prioridade a esse contrato e incluí-lo na *blockchain* (Binance, O que é Ethereum? 2019).

Ao ser possível definir um limite de *gwei*, isso serve como uma salvaguarda. Um *smart contract* pode, por algum motivo, não estar corretamente configurado e consumir mais gás do que originalmente desenhado. Ao limitar o gás, significa que no máximo irá gastar um determinado valor X. Se utilizar uma quantidade superior a X, esse contrato será interrompido (Vilaça Pacheco, 2021).

2.12.2 O que são os *token Ethereum*?

O facto de poderem ser desenvolvidas novas *blockchain* dentro da *Ethereum* e criar *tokens* fazem da *Ethereum* um projeto com imenso sucesso. Qualquer utilizador pode desenvolver um *token*, *blockchain* e *smarts contracts*. Relativamente aos *tokens*, já existem regras pré-definidas das quais algumas são personalizadas, como a quantidade de moedas a ser emitidas, se são divisíveis, se são fungíveis, entre outros. (Frankenfield, 2022)

O *ERC-20* é um protocolo que permite a qualquer utilizador criar a sua própria moedas sem necessitar de ser o detentor de uma *blockchain*, desde que cumpra os pressupostos predefinidos. Isso permite que imensas empresas criem as suas próprias criptomoedas para suportar as suas aplicações. No momento da realização desta dissertação, em setembro de 2022 existiam 662.340 *ERC-20 Token* (Binance, O que é Ethereum?, 2019).

2.12.3 A escalabilidade na *Ethereum*

Assim como a Bitcoin, a *Ethereum* tem problemas com a escalabilidade. Para suprimir essa debilidade, Vitalik projetou um novo caminho para a rede *Ethereum*. Com o constante crescimento da *blockchain*, é necessário melhorar os processos, tornando os contratos inteligentes mais autónomos, descentralizados e com foco na privacidade. Para que isso seja possível o poder de transações da rede *Ethereum* tem de aumentar exponencialmente.

Com o método de *PoW,* a rede *Ethereum* não limitava o volume de transações, como faz a rede Bitcoin, mas limitava a quantidade de *Gwei* utilizado num bloco. Por exemplo, se um bloco tem o limite de 100 *gwei*, seria possível introduzir 10 transações de 10 *gwei*, ou então 2 transações de 50 *gwei*, sem nunca exceder os limites de 100 *gwei* por bloco. Se forem introduzidas transações que excedam o limite de *gwei* nesse bloco, essas mesmas terão de aguardar que seja introduzido na rede um novo bloco valido (Buterin, 2013).

Uma vez que a *Ethereum* é uma das redes mais utilizados do mundo, essa limitação era prejudicial para a rede e para a quantidade de transações que são efetuadas diariamente. Começariam a acumular-se transações na rede, o preço do *gwei* iria aumentar e os utilizadores teriam de pagar cada vez mais para que as transações fossem aprovadas. Dependo do congestionamento da rede, algumas taxas podem ficar mais caras do que a própria transação (Binance, O que é Ethereum?, 2019).

A falha na rede *Ethereum* que afetou a escalabilidade foi descoberta em 2017, quando a popularidade dos *cryptokitties* explodiu. *O cryptokitties* é um jogo onde os usuários podem criar seus próprios avatares como gatos. O jogo levou ao congestionamento da rede durante várias horas, devido às elevadas transações que eram efetuadas por segundo. Alguns utilizadores da comunidade pediram para que a rede aumentasse a quantidade de limite de *gwei* por bloco de modo que a rede pudesse processar mais transações por bloco (Vilaça Pacheco, 2021).

A *Ethereum* sempre manteve uma média de 15 TPS enquanto utilizava o método de consenso *PoW*, o que para o objetivo de ser a maior plataforma, e de ser tonar um "computador global" é considerado relativamente baixo. No entanto, a transição para a *Ethereum* 2.0, com a utilização do algoritmo de consenso de Prova de Participação (*PoS*), deve aumentar ainda mais a capacidade da rede, permitindo a validação de até 100.000 transações por segundo através do uso de *rollups* e *sidechains*.

2.12.4 O que é a *Ethereum* 2.0?

A *Ethereum* 2.0 é a nova imagem da *Ethereum* e o seu futuro foi discutida durante vários anos. Finalmente, em 15/09/2022 aconteceu o aguardado *Merge* que acabou de vez com o método de consenso *PoW* e implementou o *PoS*. Com esta transição estimasse uma poupança de 99 % na energia utilizada pela rede, devido à sua escalabilidade. Este upgrade era algo necessário para acompanhar o crescimento diário da rede. Para que a rede continue descentralizada, foi imposto no novo processo de *POS* uma entrada mínima de 32 ETH por *pool*, para garantir a descentralização da *blockchain* (Binance, O que é Ethereum?, 2019).

No sistema *PoS* os blocos não são minerados, mas são sim forjados. Não há competição através do *hashpow*er[26]. Com o método de *PoS,* é escolhido aleatoriamente um validador para validar o bloco candidato a ser introduzido na *blockchain*. Se a validação for realizada corretamente, esse validador receberá todas as taxas de transações desse bloco. (Frankenfield, 2022)

Um dos principais motivos da transição dos métodos de consenso de *PoW* para o *PoS*, foi a consciência ambiental. Estimasse que o consumo de energia anual nos métodos *PoS* seja 99% inferior ao de *PoW*. Considerando que há uma grave crise energética, potenciou a que esta passagem de método de consenso fosse realizada com a maior brevidade possível.

2.12.5 O que é *Ethereum staking*?

Com a introdução da *Ethereum* 2.0, o método de consenso deixou de ser *PoW* e passou a *PoS*. Anteriormente a rede era assegurada pelos mineradores, mas agora é validada pela participação de cada utilizador (*stake*), que coloca as suas moedas como valor "colateral" para que a informação que eles validem, seja verdadeira. Caso haja tentativa de enganar o sistema, o utilizador perder as suas moedas. Atualmente para ser um validador no método *PoS* é necessário ter um mínimo de 32

[26] Quanto mais hashpower um minerador tivesse, maior probabilidade tinha de validar o bloco.

ETH, um valor considerável para impedir que existam agentes mal-intencionados e para prevenir um potencial ataque de 51% (Buterin, 2013).

2.12.6 O que são Finanças Descentralizadas (*DeFi*)?

As finanças descentralizadas são um projeto na *blockchain* para descentralizar o sistema financeiro e são utilizadas em *blockchains* publicas de código aberto, com a *Ethereum* a ser a principal. Atualmente existem já projetos *P2P* e aplicações decentralizadas (*DAPPS*) integram vários projetos *DeFi*.

Esses projetos permitem aos seus utilizadores o controlo dos seus fundos em um curto espaço de tempo, ao contrário dos bancos, que dependendo do montante poderá levar a dias para ser efetuado o levantamento. Resumidamente, o objetivo do *DeFi* é criar um sistema financeiro sem as falácias do atual.

Sendo o projeto *DeFi* de *open source*, e com muitos utilizadores ainda sem acesso a qualquer tipo de serviço financeiro, esta seria uma solução que poderia ser implementada em países menos desenvolvidos. Onde existe escassez de bens essências, mas onde a maioria tem acesso a um telemóvel e internet.

As *stablecoins* são um dos serviços mais populares das DeFi, ao estarem anexadas a um ativo real, o seu valor é seguro e pratico para realizar pagamentos. Outro ponto atraente das *DeFi* são os serviços *P2P*, que permitem emprestar os nossos fundos a outros utilizadores e receber juros por esse empréstimo. Plataformas como a Binance a Coinbase são das mais fortes no mercado de criptomoedas neste serviço (Binance, O que é Ethereum?, 2019).

Para além das DeFi, existem também as *exchanges* descentralizadas (*DEX*), que são plataformas que permitem aos utilizadores realizar transações diretamente entre eles, sem a necessidade de intermediários. Esse modelo só é possível graças aos contratos inteligentes, que são programas de computador que executam automaticamente as condições pré-determinadas entre as partes envolvidas em uma transação. Dessa forma, as *DEXs* são muito mais seguras e transparentes do que as exchanges centralizadas, que ficam sujeitas a ataques de *hackers* e fraudes. Alguns exemplos de *DEXs* populares são a *Uniswap* e a *Sushiswap*, que funcionam na rede *Ethereum*.

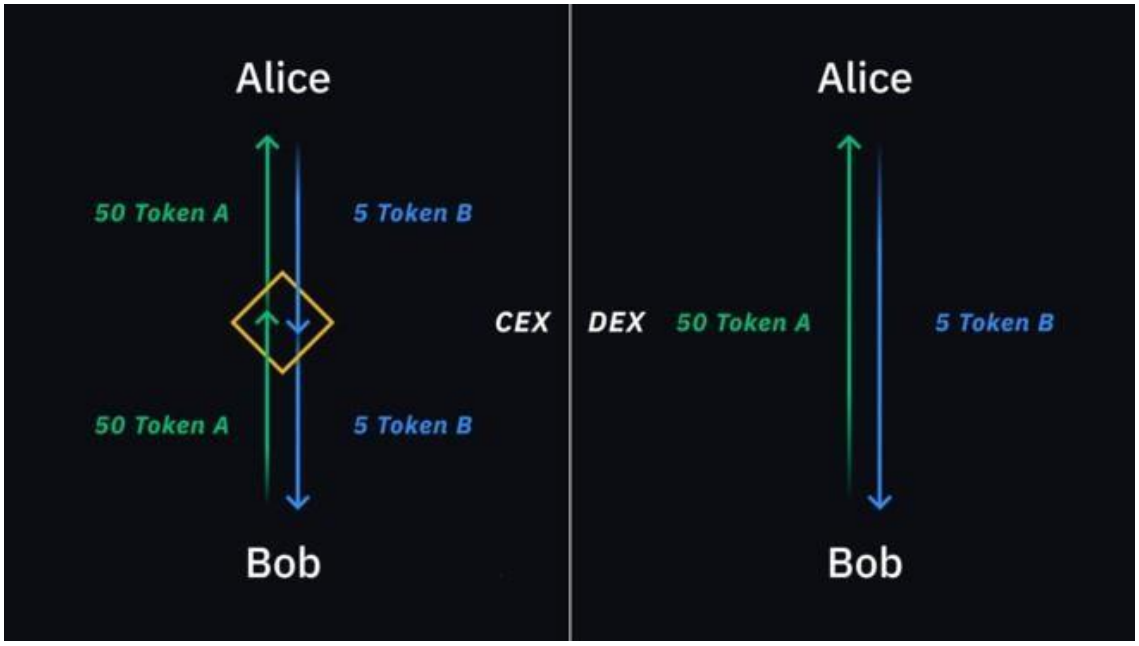

Figura 6 - *Exchanges* centralizadas *vs* descentralizadas.
Fonte: https://image.binance.vision/editor-uploads/4c23644c334d4b728b177ff23ea81774.png

Na imagem acima, podemos verificar uma comparação entre uma transação realizada através de uma plataforma centralizada (esquerda) e uma transação realizada através de uma *DEX* (direita). Na transação da esquerda, Bob envia 50 *token* A para Alice, que precisa ser validado por um intermediário. Em seguida, Alice envia 5 *token* B para Bob, que também precisa ser validado pelo intermediário antes de ser enviado para Bob. Esse processo envolve tempo e comissões inerentes.

Já na transação da direita, as operações são realizadas em uma *DEX*. Bob envia 50 *token* A para Alice em troca de 5 *token* B, sem a necessidade de intermediários. Isso é possível devido ao uso de contratos inteligentes, que garantem que a transação seja executada automaticamente, sem a necessidade de validação por um intermediário. Isso torna a transação mais rápida e barata, uma vez que não há comissões envolvidas para intermediários.

2.12.7 O que era *The DAO* e o porquê de haver a *Ethereum* Classic?

Uma vez que a *Ethereum* é uma *blockchain* de código aberto, qualquer programador pode desenvolver a sua própria criação. Ela foi uma das impulsionadoras das *DAO's* (*decentralized autonomous organization*). Um dos projetos pioneiro foi o "*The DAO*", projeto ambicioso que prometia revolucionar a *blockchain*. Foi realizada uma *ICO* em que foram distribuídos *token*s da *DAO* e deram aos seus detentores direitos de votos.

Após o incidente, que ocorreu em junho de 2016, a comunidade *Ethereum* dividiu-se sobre como lidar com o roubo. Alguns utilizadores acreditavam que a blockchain deveria ser imutável e que nenhuma alteração deveria ser feita para reverter o roubo. Outros argumentavam que a imutabilidade deveria ser flexível em situações extremas, como essa, e que uma mudança deveria ser feita para proteger os investidores.

Finalmente, foi decidido realizar um *hard fork* para reverter o roubo e devolver os fundos aos investidores prejudicados. Essa decisão foi controversa, pois violou o princípio da imutabilidade, um dos pilares da tecnologia *blockchain*. Além disso, alguns argumentaram que o *hard fork* poderia criar um precedente perigoso, tornando a *blockchain* vulnerável a intervenções arbitrárias.

No entanto, a maioria da comunidade *Ethereum* decidiu seguir em frente com o *hard fork*, e a nova rede *Ethereum* foi lançada em julho de 2016. A rede original com o ataque foi renomeada para *Ethereum Classic*, e a sua imutabilidade foi garantida. O incidente serviu como um aviso de que as tecnologias *blockchain* ainda estão em desenvolvimento e que há desafios significativos a serem superados para garantir a segurança e a confiança em sistemas descentralizados (Binance, O que é Ethereum?, 2019).

Este acontecimento, apesar de negativo foi extremamente elucidativo, pois verificou-se que não se pode confiar grandes quantidades em códigos autónomos e também para perceber como é complicado tomar decisões coletivas num ambiente aberto, como é a *blockchain*.

2.13 Como é efetuada a mineração de criptomoedas?

A mineração de criptomoedas é o processo de assegurar que as transações sejam verificadas e adicionadas ao livro-razão (*ledger*) da *blockchain*. Essas operações também originam a emissão de novas moedas. O fundador da *Bitcoin* Satoshi Nakamoto referiu que não fazia sentido num sistema de *blockchain* se eleger um júri ou um grupo de juízes, empresas ou até mesmo instituições financeiras como os bancos, este é a base do funcionamento no sistema de consenso.

No sistema convencional de base de dados, a segurança é baseada em níveis de restrição delegados a quem tem acesso. No entanto, com a *blockchain,* a segurança é assegurada por um complexo código matemático previamente desenvolvido. Esse código matemático é responsável por garantir a confiança na rede e deve encontrar um consenso com outros *miners*. Ao prestarem esse serviço, os *miners*, terão direito a uma percentagem das transações efetuadas no bloco, na moeda que validam nessa *blockchain*. Por exemplo, se estivermos a minerar *bitcoin* recebemos *bitcoin*, se estivermos a minerar *Ethereum* recebemos *Ether* (Buterin, 2013) .

A mineração de criptomoedas está associada ao rendimento passivo, ou seja, um rendimento que não exige a necessidade de dedicar tempo para obter lucro. Um exemplo de rendimento passivo é o mercado imobiliário, onde ser obtém um rendimento por alugar um imóvel a outra pessoa, que por mês irá pagar uma renda. Neste caso, não é necessário despender tempo ou esforço para obter esse rendimento. Claro que existem despesas inerentes a esse imóvel como impostos, hipoteca e condomínio (Vilaça Pacheco, 2021).

A mineração poderá ser considerada um rendimento passivo, para isso é necessário adquirir material informático para fazer construir uma *rig*, constituído por placas gráficas (*CPU*) *motherboard*, processador, *RAM*, uma fonte de alimentação, disco rígido para ter o sistema operativo.

A compra de material, é o investimento inicial no projeto, e posteriormente a única despesa é o do consumo de rede elétrica que a *rig* necessita para estar ligada 24 horas. No entanto, o custo

destes materiais tem vindo a aumentar de ano para ano, devido à enorme procura deste rendimento passivo e a escassez no mercado, agravada pela pandemia fez disparar o preço desses componentes.

Já a mineração de *bitcoin*, é atualmente efetuada através de *ASIC*, minicomputadores com uma enorme capacidade computacional enorme que permite resolver complexas equações matemáticas para minerar os blocos. Essas *ASIC* são aparelhos compactos, porém tem um consumo elétrico elevado e aquecem muito. Estas *farm's* de *ASIC* estão localizadas em países com um clima frio e situadas em armazéns já preparados para acolher estes "minicomputadores", alguns utilizadores já recorrem a energias renovadas, como hidráulicas e eólicas para assegurar a energia (Vilaça Pacheco, 2021).

2.14 Diferentes métodos de mineração de criptomoedas

2.14.1 Mineração via CPU

Este tipo de mineração foi muito popular no início das criptomoedas, quando a dificuldade era baixa, utilizado o CPU do computador. Um CPU fraco era capaz de minerar muitas *Bitcoin*s em 2010, mas ficou obsoleto à medida que cada vez mais pessoas começaram a juntar-se à rede. O aumento da dificuldade e do *hash*rate (Cong & He, 2018), levou a que este método fosse facilmente ultrapassado. Nem os melhores CPU do momento, como por exemplo, um i9 de última geração da Intel, são viáveis para minerar criptomoedas devido à dificuldade da rede (Vilaça Pacheco, 2021).

2.14.2 Mineração via GPU

Esta é mineração mais utilizadas nos dias de hoje, a mineração de GPU, também conhecida por placas gráficas. São utilizadas maioritariamente em videojogos e programas que necessitam elevada capacidade gráfica A elevada memoria que possuem torna-as uma solução viável para minerar criptomoedas. Foram utilizadas para minerar *Ethereum* e outras criptmoedas, uma vez que já não é viável minerar *Bitcoin* com GPU, pois o consumo de energia supera o benefício (Vilaça Pacheco, 2021).

2.14.3 Mineração ASIC

As *ASIC (Application-Specific Integrated Circuits*), foram criadas exclusivamente para minerar *Bitcoin* (Zola, 2021). Este é o melhor sistema de mineração. No entanto, para além da aquisição ter um custo elevado, tem um consumo energético alto. São máquinas que produzem muito calor e precisam de estar em ambientes atmosfericamente controlados. Além disso, são máquinas altamente competitivas e ficam rapidamente ultrapassadas, havendo a necessidade de estar sempre a trocar os modelos antigos por recentes para obter o maior lucro possível. Alguns equipamentos chegam a custar por volta de 15.000 €.

Através destes aparelhos os mineradores conseguem minerar os blocos, mas para isso têm de ser os primeiros a conseguir encontrar o *hash* correto para esse bloco. Se for um minerador sozinho essa probabilidade é muito baixa Os mineradores recorrem aos "pools de mineração"

3. Metodologia e análise empírica

Neste capítulo, dividido em três partes, são apresentados os resultados obtidos no estudo empírico realizado nesta investigação, de acordo com as metodologias estatísticas usadas. Na primeira parte será analisada a rendibilidade diárias das três amostras de estudo: o *SP500*, a *Bitcoin* e a *Ethereum*. Serão utilizados os anos de 2019, 2020 e 2021. bem como o primeiro semestre de 2022. A metodologia estatística utilizada para analisar as correlações entre as três amostras foi correlação de Pearson e de Spearman.

Na segunda parte, analisa-se a emissão dos *smarts contracts* e como afetam o preço da *Ethereum*, investigando-se se a variação diária da quantidade de *smarts contracts* emitidos afeta o preço diário da *Ethereum*. Será feita também uma comparação entre a variação percentual de *smarts contracts* emitidos e a rendibilidade diária de *Ethereum*. Os métodos de analise estatística utilizados foram a correlação de Pearson e a regressão linear simples.

Na terceira e última parte, recorre-se à análise gráfica para verificar se a variação percentual do preço médio mensal das três amostras: SP500, *Bitcoin* e *Ethereum*, ao longo do tempo é afetada por fatores macroeconómicos.

3.1 Rentabilidade anual *SP500, Bitcoin e Ethereum*

Rendibilidade 2022

	N	Mínimo	Máximo	Média	Desvio padrão	Variância	Assimetria		Curtose	
	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Erro Padrão	Estatística	Erro Padrão
SP500	124	-4,07%	3,32%	-0,2227%	1,48761%	2,213	-,407	,217	-,153	,431
Bitcoin	180	-18,04%	12,44%	-0,4968%	3,70807%	13,750	-,777	,181	4,030	,360
Ethereum	180	-19,01%	11,96%	-0,7397%	4,69606%	22,053	-,933	,181	2,785	,360
N válido (de lista)	124									

Tabela 1 - Rendibilidade 2022.
Fonte: Elaboração própria.

A rendibilidade do *SP500* foi baseada em uma amostra estatística de 124 dias, devido ao facto de o índice replicar as 500 melhores empresas cotadas nos Estados Unidos da América e a bolsa americana está aberta somente de segunda a sexta-feira. A rendibilidade de 2022 foi calculada utilizando os primeiros seis meses do ano, nos quais o *SP500* teve um mínimo estatístico negativo de (4.07%) e um máximo de 3.22%. A média estatística fixou-se negativamente em

(0.22%). O desvio Padrão é de 1.48 %, que corresponde ao valor de dispersão em torno da média. Em relação à assimetria como podemos observar na tabela Rendibilidade 2022, na variável *SP500*, o valor está entre -1.96 e 1.96 (-,407), portanto, a assimetria não deverá ser rejeitada. No que diz respeito à análise da medida de achatamento, o valor da curtose está entre -1.96 e 1.96 (-,153), logo estaremos perante uma curva normal.

Já a *Bitcoin*, nos primeiros seis meses de 2022, assim como a *Ethereum,* teve uma amostra de 180 dias, uma vez que não tem restrições como o *SP500*, existe transações todos os dias. A Bitcoin teve uma rendibilidade diária mínima negativa de (18.04%), um valor máximo de 12.44%, com uma média estatística negativa de (0.49%). O desvio padrão é de 3.70 % correspondendo ao valo ao valor de dispersão em torno da média. A assimetria tem um valor de -,777, logo não deverá ser rejeitada. Em relação à curtose, o valor é de 4.03, o que indica uma curva alongada.

Por fim, até ao final de junho de 2022, a *ethereum* teve uma rendibilidade mínima diário negativa de (19.01%), atingindo um máximo de 11.96 %, com uma média negativa diária de (0.73%). A *ethereum* teve o desvio padrão mais elevado das três comparações, fixando-se nos 4.69%. A assimetria não pode ser rejeitada por ser de, -933, enquanto a curtose é de curva alongada por ser superior a 1.96, com o valor de 2.78.

Os valores das criptomoedas são mais dispersos, conforme revela o desvio padrão e a variância estatística, porque são ativos com uma elevada volatilidade, ao contrário do *SP500*.

Correlações Pearson 2022

		SP500	Bitcoin	Ethereum
SP500	Correlação de Pearson	1	,041	-,032
	Sig. (2 extremidades)		,650	,728
	N	124	124	124
Bitcoin	Correlação de Pearson	,041	1	,904**
	Sig. (2 extremidades)	,650		<,001
	N	124	180	180
Ethereum	Correlação de Pearson	-,032	,904**	1
	Sig. (2 extremidades)	,728	<,001	
	N	124	180	180

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 2- Correlações Pearson 2022.
Fonte: Elaboração própria.

A correlação de Pearson entre o *SP500* e *Bitcoin* é de .041, já a *SP500* e *Ethereum* é negativa em (,032). O nível de significância estatística é de ,650 para a correlação entre o *SP500* e *Bitcoin* e de .728 para a correlação entre o *SP500* e *Ethereum*. Não há significância estatística para concluir que há correlação entre a variável *SP500* e as demais criptmoedas.

Já a *Bitcoin* apresenta uma correlação de Pearson alta com a *Ethereum* de ,904 e um nível de relevância estatística significativo, uma vez que o Sig é inferior a 0.01, indicando uma correlação positiva forte (ou seja, quando uma aumenta, a outra também aumenta linearmente), devido à alta volatilidade partilhada por as criptmoedas.

Correlações Spearman 2022

			SP500	Bitcoin	Ethereum
rô de Spearman	SP500	Coeficiente de Correlação	1,000	,081	,012
		Sig. (2 extremidades)	.	,370	,899
		N	124	124	124
	Bitcoin	Coeficiente de Correlação	,081	1,000	,902**
		Sig. (2 extremidades)	,370	.	<,001
		N	124	180	180
	Ethereum	Coeficiente de Correlação	,012	,902**	1,000
		Sig. (2 extremidades)	,899	<,001	.
		N	124	180	180

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 3 - Correlações Spearman 2022.
Fonte: Elaboração própria.

Tal como acontece na correlação de Pearson, o rô de Spearman também indica um coeficiente de correlação baixo entre o *SP500* e a *Bitcoin* de 0.81 e de 0.12 com a *Ethereum*. No entanto, essas duas correlações não têm significância estatista, uma vez que o nível de significância (Sig) é de ,370 para o *SP500* e *Bitcoin* e de ,899 para o *SP500* e *Ethereum*.

Já a *Bitcoin* apresentou uma correlação de Spearman significativa de ,902 com a *Ethereum*, tendo um nível de significância estatística inferior a 0.01. Isso ocorre porque essas duas variáveis são voláteis, ao contrário dos *SP500* que é um índice considerado estável em comparação com as criptomoedas.

Rendibilidade 2021

	N	Mínimo	Máximo	Média	Desvio padrão	Variância	Assimetria		Curtose	
	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Erro Padrão	Estatística	Erro Padrão
SP500	249	-5,51%	2,99%	0,1065%	0,91210%	,832	-1,129	,154	6,126	,307
Bitcoin	365	-16,35%	15,78%	0,0686%	4,22661%	17,864	-,304	,128	1,709	,255
Ethereum	365	-38,06%	20,51%	0,3005%	5,71610%	32,674	-1,076	,128	6,633	,255
N válido (de lista)	249									

Tabela 4- Rendibilidade 2021.
Fonte: Elaboração própria.

Em 2021, O SP500 teve uma rendibilidade mínima negativa de (5.51%), atingindo uma rendibilidade máxima de 2.99%, com a média de 0.10 %. Apresentou uma assimétrica negativa de (1.129), valor pelo qual não se deve rejeitar a simetria. Já a curtose apresenta uma curva alongada.

A *Bitcoin* apresentou em 2021 um mínimo estatístico negativo de (16.35%) e um máximo estatístico de 15.78%, com uma média estatística de apenas 0.06%. O desvio padrão foi de 4.22%, a assimetria teve um valor de (,304) mas não se rejeita a simetria. A curtose de 1.709 revela uma curva normal.

A *Ethereum* teve os valores mais dispersos das três amostras, com uma rendibilidade mínima estatística negativa de (38.06%) atingido um máximo de 20.51 %, com a média estatística mais elevada das três amostras de 0.30 %. A uma assimetria negativa foi de (1.076), a curtose revela uma curva alongada. Estes valores refletem o *bull market* que ocorreu no ano de 2021, permitindo que o índice do SP500 e as duas criptomoedas atingissem valores máximos históricos, com a *Bitcoin* a chegar aos 57.000 €.

Correlações Pearson 2021

		SP500	Bitcoin	Ethereum
SP500	Correlação de Pearson	1	,041	,055
	Sig. (2 extremidades)		,522	,385
	N	249	249	249
Bitcoin	Correlação de Pearson	,041	1	,787**
	Sig. (2 extremidades)	,522		<,001
	N	249	365	365
Ethereum	Correlação de Pearson	,055	,787**	1
	Sig. (2 extremidades)	,385	<,001	
	N	249	365	365

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 5 - Correlações Pearson 2021.
Fonte: Elaboração própria.

A correlação de Pearson entre o *SP500* e *Bitcoin* é de .041, enquanto a correlação entre o *SP500* e *Ethereum* é de ,055. O nível de significância estatístico é de ,522 para o *SP500* e *Bitcoin* e .385 para o *SP500* e *Ethereum*. que significa que não há significância estatística para concluir que há correlação entre o índice *SP500* e as outras criptomoedas.

Já a *Bitcoin* apresenta uma correlação de Pearson alta com a *Ethereum* de ,787 e um nível de relevância estatística significativo, uma vez que o Sig é inferior a 0.01. Isso indicando uma correlação positiva forte, devido à alta volatilidade partilhada pelas criptmoedas.

Correlações Spearman 2021

			SP500	Bitcoin	Ethereum
rô de Spearman	SP500	Coeficiente de Correlação	1,000	-,022	,021
		Sig. (2 extremidades)	.	,727	,744
		N	249	249	249
	Bitcoin	Coeficiente de Correlação	-,022	1,000	,766**
		Sig. (2 extremidades)	,727	.	<,001
		N	249	365	365
	Ethereum	Coeficiente de Correlação	,021	,766**	1,000
		Sig. (2 extremidades)	,744	<,001	.
		N	249	365	365

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 6 - Correlações Spearman 2021.
Fonte: Elaboração própria.

O *SP500* no ano de 2021 teve um coeficiente de correlação de Spearman negativo de (,022) com a *Bitcoin* e de 0,21 com a *Ethereum*. No entanto, estas duas variáveis não apresentaram significância estatista, visto que o Sig. foi de ,727 para a correlação entre o *SP500* e *Bitcoin* e de ,744 para a correlação entre o *SP500* e *Ethereum*. Por sua vez, a *Bitcoin* apresentou uma correlação de Spearman com a *Ethereum* de ,766, tendo o Sig relevância estatística por ser inferior a 0.01.

Rendibilidade 2020

	N	Mínimo	Máximo	Média	Desvio padrão	Variância	Assimetria		Curtose	
	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Erro Padrão	Estatística	Erro Padrão
SP500	251	-7,40%	5,86%	0,0443%	1,58922%	2,526	-,768	,154	3,498	,306
Bitcoin	366	-56,63%	17,59%	0,2667%	4,33414%	18,785	-6,020	,128	81,610	,254
Ethereum	366	-71,63%	18,25%	0,30%	5,74%	33,043	-5,401	,128	67,239	,254
N válido (de lista)	251									

Tabela 7- Rendibilidade 2020.
Fonte*:* Elaboração própria*.*

A rendibilidade de 2020 foi fortemente afetada pela pandemia à escala global, o vírus do Covid-19. Isso refletiu-se na rendibilidade mínima negativa de (7.40%) para o *SP500*, (56.63%) para a *Bitcoin* e (71.63%) para a *Ethereum*, enquanto a rendibilidade máxima atingiu apenas 5.86 % no *SP500*, 17.59% na *Bitcoin* e 18.25% na *Ethereum*. Como são ativos com elevada volatilidade, as criptomoedas foram os ativos que sofreram mais com a crise provocada pela pandemia.

O desvio padrão do *SP500*, devido ao facto de não ter tanta volatilidade como as criptomoedas situou-se em 1.58% A *Bitcoin* atingiu 4.33%, sendo superada pela *Ethereum* com um elevado desvio padrão de 5.74%.

A Assimetria do *SP500* não deve ser rejeitada, enquanto a *Bitcoin* e *Ethereum* apresentaram assimetria negativa, com valores de (6.02) para a *Bitcoin* e (5.401) para a *Ethereum*. Isso indica uma maior concentração de observações na cauda esquerda da distribuição e que as rendibilidades negativas são mais frequentes do que as rendibilidades positivas. Esse facto pode ser explicado pelo elevado valor mínimo atingido por ambas as criptomoedas em 2020.

Já os valores de curtose são elevados (3.498 para o *SP500*; 81,61 para a *Bitcoin*; 67,239 para a *Ethereum*), indicando que a curva alongada tem uma distribuição leptocúrtica, ou seja, apresentam picos mais acentuados e uma concentração maior de observações em torno da média, em comparação com uma distribuição normal. Isso indica um maior risco associado aos ativos, especialmente à *Bitcoin* e à *Ethereum*, devido à sua maior volatilidade.

Correlações Pearson 2020

		SP500	Bitcoin	Ethereum
SP500	Correlação de Pearson	1	-,076	-,119
	Sig. (2 extremidades)		,228	,060
	N	251	251	251
Bitcoin	Correlação de Pearson	-,076	1	,892**
	Sig. (2 extremidades)	,228		<,001
	N	251	366	366
Ethereum	Correlação de Pearson	-,119	,892**	1
	Sig. (2 extremidades)	,060	<,001	
	N	251	366	366

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 8 - Correlações Pearson 2020.
Fonte: Elaboração própria.

A correlação de Pearson entre o *SP500* e *Bitcoin* é negativa em (,076), enquanto a correlação entre o *SP500* e *Ethereum*, é também negativo em (,119) com um nível de significância estatístico de ,228 entre o *SP500* e *Bitcoin* e .060 entre o *SP500* e *Ethereum*. Por outro lado, a *Bitcoin* apresenta uma alta correlação de Pearson com a *Ethereum* de ,892, com um nível de relevância estatística, uma vez que o *Sig* é inferior a 0.01.

Correlações Spearman 2020

			SP500	Bitcoin	Ethereum
rô de Spearman	SP500	Coeficiente de Correlação	1,000	-,089	-,153*
		Sig. (2 extremidades)	.	,158	,015
		N	251	251	251
	Bitcoin	Coeficiente de Correlação	-,089	1,000	,806**
		Sig. (2 extremidades)	,158	.	<,001
		N	251	366	366
	Ethereum	Coeficiente de Correlação	-,153*	,806**	1,000
		Sig. (2 extremidades)	,015	<,001	.
		N	251	366	366

*. A correlação é significativa no nível 0,05 (2 extremidades).

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 9 - Correlações Spearman 2020.
Fonte: Elaboração própria.

O *SP500* no ano de 2020 teve um coeficiente de correlação de Spearman negativo de (,089) com a *Bitcoin* e também negativo em (,153) com a *Ethereum*. No entanto, essas duas variáveis não apresentam significância estatista, pois entre o *SP500* e *Bitcoin* existe um *Sig*. de ,158 e com a *Ethereum* de ,015.

A *Bitcoin* no ano de 2020 teve uma correlação de Spearman com a *Ethereum* de ,806, tendo o *Sig* relevância estatística por ser inferior a 0.01.

Rendibilidade 2019

	N	Mínimo	Máximo	Média	Desvio padrão	Variância	Assimetria		Curtose	
	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Estatística	Erro Padrão	Estatística	Erro Padrão
SP500	251	-3,65%	2,42%	0,0901%	0,72458%	,525	-,707	,154	2,956	,306
Bitcoin	365	-16,59%	14,82%	0,1172%	3,52800%	12,447	-,103	,128	4,531	,255
Ethereum	365	-20,27%	13,51%	-0,0964%	4,21818%	17,793	-,767	,128	4,276	,255
N válido (de lista)	251									

Tabela 10 - Rendibilidade 2019.
Fonte: Elaboração própria.

O ano de 2019 foi um ano relativamente normal em termos económicos para as criptomoedas, que apresentavam um crescimento aceitável e estavam cada vez mais a ganhar popularidade e a confiança dos investidores.

Em termos de rendimento mínimo, o *SP500*, a *Bitcoin* e a *Ethereum* obtiveram negativamente os seguintes valores, (3.65%), (16.59%) e (20.27%), com o *SP500* a alcançar um máximo de 2.42%. A *Bitcoin* obteve 14.82% e a *Ethereum* 13.51%. A média estatística foi de 0.09 % para o *SP500* e 0.11% para a *Bitcoin*, enquanto a *Ethereum* teve uma média estatística negativa de (0.09%). A assimetria estatística foi similar para o *SP500* e *Ethereum* com uma assimetria negativa de (,707) e (,767) respetivamente. Enquanto a *Bitcoin* teve uma assimetria negativa de (,103). A curtose relevou uma curva alongada para as três amostras.

Correlações Pearson 2019

		SP500	Bitcoin	Ethereum
SP500	Correlação de Pearson	1	-,079	-,107
	Sig. (2 extremidades)		,214	,092
	N	251	251	251
Bitcoin	Correlação de Pearson	-,079	1	,836**
	Sig. (2 extremidades)	,214		<,001
	N	251	365	365
Ethereum	Correlação de Pearson	-,107	,836**	1
	Sig. (2 extremidades)	,092	<,001	
	N	251	365	365

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 11 - Correlações Pearson 2019.
Fonte: Elaboração própria.

A correlação de Pearson entre o *SP500* e *Bitcoin* é negativa em (,079), enquanto entre o *SP500* e *Ethereum*, é negativa em (,107). O nível de significância estatístico de ,214 entre o *SP500* e *Bitcoin* é .092 entre o SP500 e *Ethereum*. A *Bitcoin* apresenta uma correlação de Pearson alta com a *Ethereum* de ,836 com um nível de relevância estatística, uma vez que o Sig é inferior a 0.01.

Correlações Spearman 2019

			SP500	Bitcoin	Ethereum
rô de Spearman	SP500	Coeficiente de Correlação	1,000	-,114	-,128*
		Sig. (2 extremidades)	.	,072	,044
		N	251	251	251
	Bitcoin	Coeficiente de Correlação	-,114	1,000	,812**
		Sig. (2 extremidades)	,072	.	<,001
		N	251	365	365
	Ethereum	Coeficiente de Correlação	-,128*	,812**	1,000
		Sig. (2 extremidades)	,044	<,001	.
		N	251	365	365

*. A correlação é significativa no nível 0,05 (2 extremidades).

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 12 - Correlações Spearman 2019.
Fonte: Elaboração própria.

Em 2019, o índice *SP500* apresentou um coeficiente de correlação de Spearman negativo de (,114) com a *Bitcoin e* também negativo de (,128) com a *Ethereum*. No entanto, essas duas variáveis não têm significância estatista, pois entre o *SP500* e *Bitcoin* existe um *Sig*. de ,072 e com a *Ethereum* de ,044.

Por outro lado, a correlação de Spearman entre a *Bitcoin* e a *Ethereum* em 2019 foi de 0,812, o que indica uma correlação forte entre essas duas variáveis e um valor de *Sig*. estatisticamente significativo, com um valor inferior a 0,01. Vale ressaltar que esses dados são influenciados pela alta volatilidade das criptomoedas, em comparação com o *SP500*, que é considerado um índice mais estável.

3.2 Correlações de Pearson e regressão linear simples para quantidade de *smarts contracts* e rendibilidade da *Ethereum*

Correlação entre variação diária contratos emitidos e rendibilidade diária *Ethereum*

		Variação diária contratos emitidos	Rendibilidade diária Ethereum
Variação diária contratos emitidos	Correlação de Pearson	1	-,020
	Sig. (2 extremidades)		,487
	N	1277	1271
Rendibilidade diária Ethereum	Correlação de Pearson	-,020	1
	Sig. (2 extremidades)	,487	
	N	1271	1271

Tabela 13- Correlação entre variação diária contratos emitidos e rendibilidade diária *Ethereum*.
Fonte: Elaboração própria.

A amostra utilizada para a análise estatística consistiu na variação diária de *smarts contracts* emitidos, comparada com a rendibilidade diária da *Ethereum*. Foi utilizada a métrica de correlação de Pearson, cujo objetivo é medir o grau de correlação entre duas variáveis de escala métrica.

A correlação Pearson entre a variação diária *smarts contracts* emitidos é negativa em (,020) onde existe uma correlação negativa desprezível. Além disso, o grau de significância é superior a 0,05, o que revela que não existe relevância estatística entre as duas amostras. O valor estatístico entre as variáveis é de ,487.

Correlação entre quantidade *smarts contracts* emitidos diariamente e preço diário *Ethereum*

		Quantidade *smarts contracts* emitidos diariamente	Preço diário Ethereum
Quantidade *smarts contracts* emitidos diariamente	Correlação de Pearson	1	-,161**
	Sig. (2 extremidades)		<,001
	N	1278	1275
Preço diário Ethereum	Correlação de Pearson	-,161**	1
	Sig. (2 extremidades)	<,001	
	N	1275	1275

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 14 -Correlação entre quantidade *smarts contracts* emitidos diariamente e preço diário *Ethereum*.
Fonte: Elaboração própria.

A amostra utilizada nesta análise estatística foi a quantidade diária de *smarts contracts* emitidos e a variação diária do preço da *Ethereum*. Observou-se uma correlação negativa moderada de (,161), que se deve ao facto de que quanto mais *smarts contracts* são emitidos, mais *gweis*[27] são necessários para validar todos os *smarts contracts*. As taxas precisam ser cada vez mais elevadas para validar o contrato, o que faz com que o preço da moeda baixe para tentar diminuir o custo da verificação dos *smarts contracts*.

Além disso, existe significância estatística entre essas duas variáveis, com um Sig inferior a 0,01. Verifica-se que as duas variáveis estão interligadas, de modo que a variação de uma afeta a outra.

Regressão linear simples – Rendibilidade diária *Ethereum*

Modelo		Coeficientes não padronizados B	Coeficientes não padronizados Erro Erro	Coeficientes padronizados Beta	t	Sig.
1	(Constante)	-,003	,151		-,020	,984
	Variação diária contratos emitidos	-,001	,002	-,020	-,695	,487

a. Variável Dependente: Rendibilidade diária *Ethereum*

Tabela 15 Regressão linear simples - Rendibilidade diária Ethereum. Fonte: Elaboração própria.

[27] *Gwei* é uma taxa cobrada para utilizar a rede *Ethereum*.

Então, o coeficiente de correlação entre a rendibilidade diária da *Ethereum* e a variação diária de contratos emitidos é negativo em (,020), o que indica que há uma correlação negativa desprezível entre as duas variáveis. No entanto, é importante notar que não há significância estatística entre elas, uma vez que o valor p é superior a 0,01. Em outras palavras, não podemos afirmar com confiança que a variação diária de contratos emitidos está relacionada com a rendibilidade diária da *Ethereum*.

3.3 Analise variação percentual preço médio

Variação percentual preço médio 2022

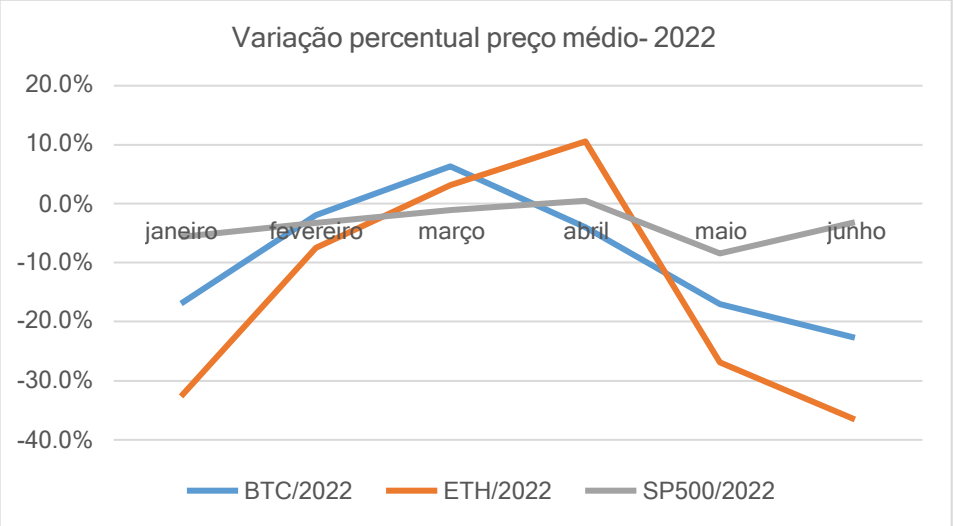

Figura 7 - Variação percentual preço médio mensal 2022.
Fonte: Elaboração própria.

O *bear market* de 2021 prolongou-se até ao final de fevereiro de 2022, tendo havido uma recuperação nas criptomoedas de mais de 30%. Numa altura em que as criptomoedas estavam a recuperar do *bear market*, em meados de fevereiro, houve a invasão da Rússia à Ucrânia. Apesar de ser um evento que poderia afetar os mercados globais, o mesmo não se verificou, muito por causa do otimismo dos mercados e dos investidores de que o conflito seria resolvido rapidamente através da paz.

Passados sete meses, verificamos que ainda não foi possível chegar a um acordo entre ambas as partes e que, a nível económico, o conflito afetou o mundo inteiro. As sanções impostas à Rússia tinham como objetivo enfraquecer o país economicamente, algo que não se verificou, apesar de ter ocorrido uma desvalorização rápida do Rublo, que foi, no entanto, recuperada rapidamente. A Rússia é um dos maiores exportadores de cereais, madeira, ferro e gás, a par da Ucrânia, o que afetou, a nível mundial, as cadeias de abastecimento e as indústrias que dependiam dessas matérias-primas.

Este confronto teve um impacto muito grave a nível mundial. Com o aumento dos preços e da inflação, colocou em risco muitos investimentos. Esse efeito foi sentido dois meses depois do conflito, em meados de abril, com o índice do *SP500* a baixar cerca de (6%). A *Bitcoin* teve uma

queda de cerca de (20%) e a *Ethereum* teve uma diminuição mais acentuada na sua rendibilidade, com uma queda de cerca de (30%).

Variação percentual preço médio 2021

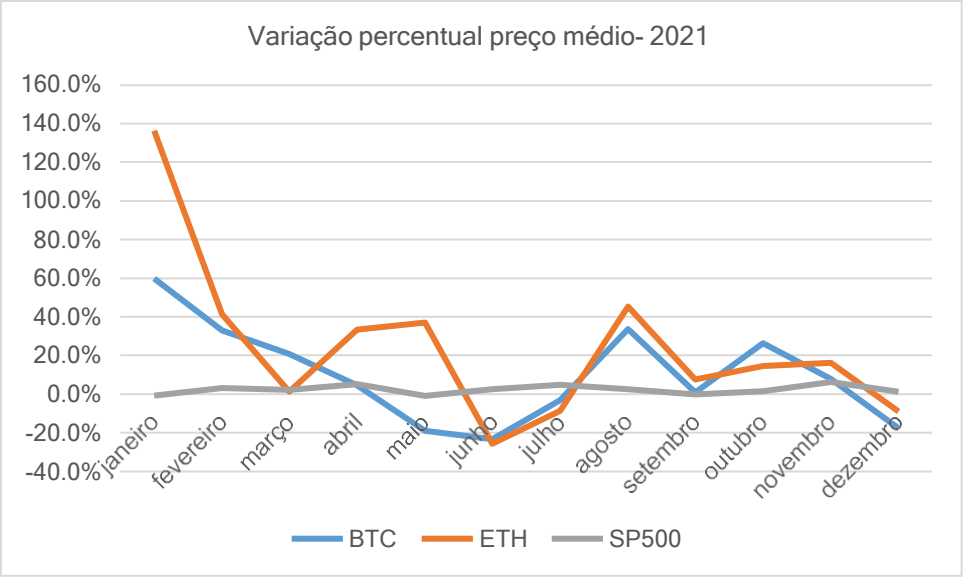

Figura 8 - Variação percentual preço médio mensal 2021.
Fonte: Elaboração própria.

O ano de 2021 era esperado que seguisse o crescimento observado em 2020. No entanto, como aconteceu em Portugal e em outros países, houve a necessidade de entrar novamente em confinamento, como ocorreu em março de 2020, o que provocou uma regressão económica. Somente os serviços essenciais estavam em funcionamento e a economia teve de parar mais uma vez.

Uma medida que afetou gravemente a variação do mercado das criptomoedas foi a necessidade de entrar novamente em confinamento, tal como aconteceu em março de 2020 em Portugal. Esse confinamento provocou uma regressão económica, com apenas os serviços essenciais a funcionar e a economia a parar mais uma vez. Isso refletiu nas criptomoedas, com a *Ethereum* a ter uma queda de 140% no primeiro trimestre e a *Bitcoin* perto de 60%. No entanto, após o final do primeiro trimestre e com a introdução das vacinas, os governos foram abrindo a economia e as criptomoedas recuperaram em parte a desvalorização do primeiro trimestre. O ano de 2021 foi um ano de altos e baixos, com a *Bitcoin* e a *Ethereum* a atingir sua maior cotação de sempre, com a *Bitcoin* quase alcançando o valor de 60.000 € e a *Ethereum* ultrapassando os 4.000 €.

No último trimestre do ano, houve então o início de mais um *bear market*, com as criptomoedas sofrendo uma desvalorizar de mais de 20 %.

Variação percentual preço médio 2020

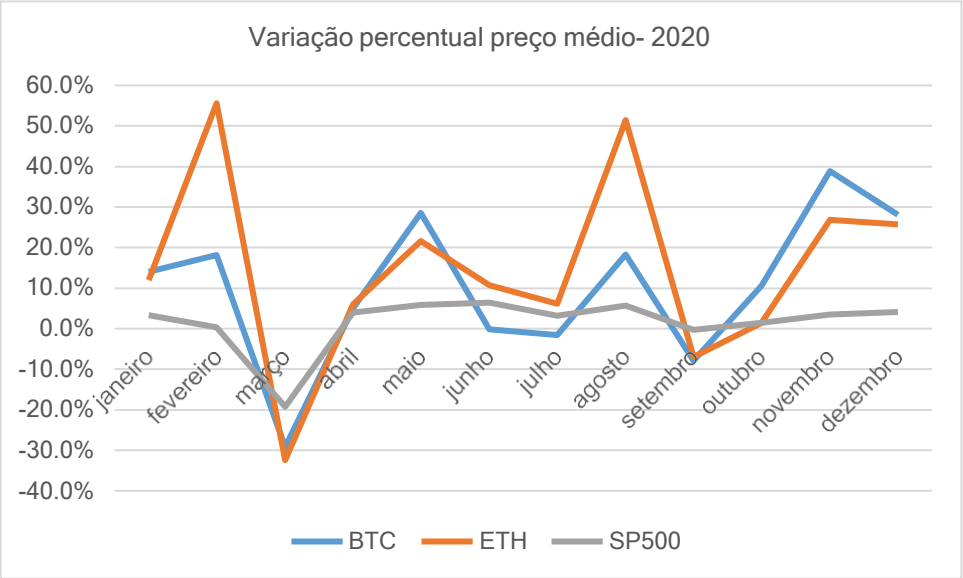

Figura 9 - Variação percentual preço médio mensal 2020.
Fonte: Elaboração própria.

2020 foi um dos anos mais desafiantes para a humanidade, um ano que começou com uma perspetiva econômica elevada, assim como foi em 2019. O projeto *Ethereum* valorizou logo 50%. No entanto, em março de 2020, a Organização Mundial de Saúde declarou a pandemia global de coronavírus, que obrigou o mundo a parar e repensar a forma como vivemos.

Em fevereiro e março de 2020, numa tentativa de conter a propagação do coronavírus, muitos governos encerraram a economia, mantendo somente os serviços essenciais em funcionamento. Estas medidas resultaram num decréscimo na variação mensal em torno dos 20% para o índice *SP500*, que foi ainda mais elevado em outros produtos financeiros. A *Bitcoin* teve uma queda de quase 40%, enquanto a *Ethereum* foi a mais afetada, com uma descida de mais de 80% na sua variação percentual.

Perante este decréscimo, o mercado financeiro entrou em *bear market*, que ficou conhecido no mundo das criptomoedas como o *Coronacrash*. Acompanhando os mercados financeiros e os principais índices, tornou-se o *bear market* mais rápido da história. No início de abril, a recuperação da variação percentual foi superior à perda inicial e houve um *bull market* durante o resto do ano, com a *Ethereum* tendo um desempenho superior ao da *Bitcoin*. Já o índice do *SP500* estabilizou seu crescimento econômico perto dos 5%.

Variação percentual preço médio 2019

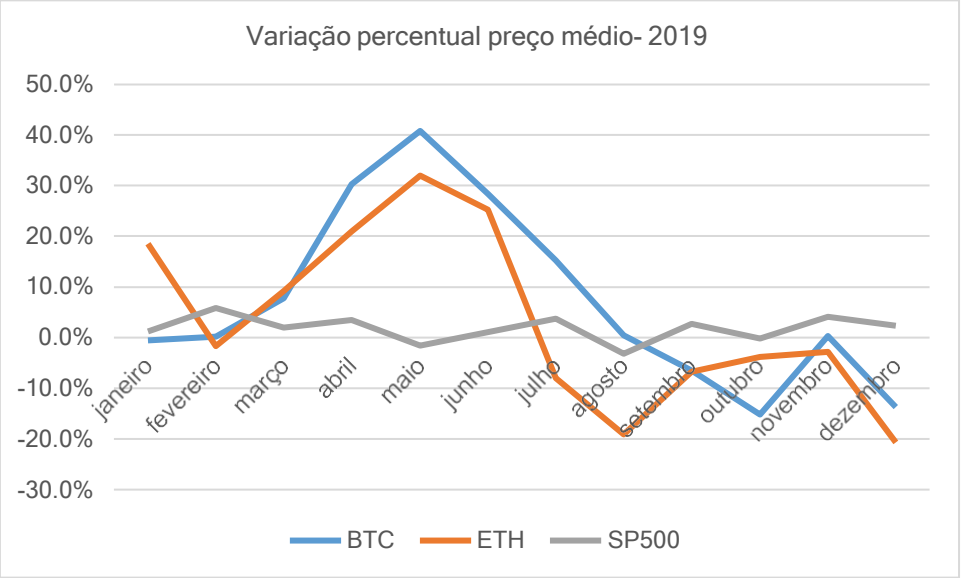

Figura 10 - Variação percentual preço médio mensal 2019.
Fonte: Elaboração própria.

No ano de 2019, um ano com perspetivas económicas muito positivas, tanto a *Ethereum* como a *Bitcoin* registaram crescimento em todos os meses, desde o início do ano até junho. A variação percentual da *Ethereum* registou uma ligeira queda no início de janeiro, mas recuperou rapidamente.

O período de *bull market* que ocorreu a partir de março deveu-se ao facto da popularidade e reconhecimento que as criptomoedas estavam a ganhar a nível mundial por parte dos investidores, com alguns projetos a ganharem maturidade, aliados à perspetiva económica positiva que se estava a sentir. Durante o terceiro trimestre, houve um decréscimo na variação mensal, que foi estabilizado no último trimestre do ano.

4. Conclusão

Um dos objetivos desta dissertação foi dar a conhecer a tecnologia *blockchain* ao público em geral, em que a revisão da literatura efetuada centrou-se na *blockchain* e nas principais criptomoedas. A *blockchain* ao ser uma rede distribuída e descentralizada, permite que a sua aplicação prática seja quase ilimitada. Uma tecnologia capaz de mudar o mundo, desde que seja devidamente utilizada, importante para salvaguardar dados importantes, como são os registos financeiros, podendo também ser aplicada à *supply chain* e à saúde (Wright & Pilippi, 2015).

São múltiplas as suas aplicações, alterando a forma como as pessoas e empresas analisam as bases de dados, podendo ser usada em qualquer setor de uma empresa ou organização. Pode também ajudar a salvar vidas humanas devido à sua utilização nos sistemas de saúde de países subdesenvolvidos, onde por vezes é difícil guardar a informação dos seus cidadãos, como o cartão de cidadão ou outros dados relacionados com saúde. Ao ficar tudo agregado na *blockchain*, os dados não seriam perdidos e poderia ajudar imenso as populações desses países (Vilaça Pacheco, 2021).

Apesar de atualmente atravessar um momento de constante desvalorização financeira, o mercado total de criptomoedas está avaliado em pouco mais de um trilião de dólares, tendo atingido em novembro de 2021, quase três triliões de dólares investidos. Tal como os mercados financeiros, as criptomoedas registaram uma acentuada desvalorização no ano de 2022. O aumento das taxas de juros e o pânico nos investidores foram os principais motivos para esta quebra. O ano de 2023 será um ano determinante para este mercado assim como 2024 pois, conforme descrito anteriormente, será um novo ciclo de *halving* da *Bitcoin*, que em anos transatos trouxe enorme valorização ao mercado das criptomoedas na sua globalidade.

Vários países estão a abraçar cada vez mais as criptomoedas e trabalham arduamente para as "legalizar" e as internalizar nos seus sistemas financeiros. Uma tarefa nada fácil e que demorará certamente alguns anos, por ser uma tecnologia nova e complexa. Um exemplo é o de El Salvador, que vivia enormes dificuldades financeiras por inúmeras razões económicas, sendo uma das mais importantes, a constante desvalorização da sua moeda. Ao decidir reconhecer a *Bitcoin* como a sua moeda, e realizar os pagamentos e recebimentos com esta criptomoeda, El Salvador poderá ser um dos primeiros países onde as criptomoedas terão impacto no crescimento económico e no funcionamento do sistema financeiro. Em países menos desenvolvidos, com economias débeis, as criptomoedas poderão ser a solução (Vilaça Pacheco, 2021).

Ao longo dos anos, o dinheiro sofreu diversas mudanças, passando da troca de gado, por metais preciosos, e atualmente por notas impressas, cartões de crédito e de débito, ainda é cedo para augurar as criptomoedas como a próxima forma de pagamento, mas aliadas à tecnologia *blockchain*, poderão ser, num futuro próximo, mais um dos inúmeros meios de pagamento viáveis e seguros que a *blockchain* proporciona (Vieira, 2017). Isto apesar do sistema financeiro institucional e os governos de diferentes países não apoiarem o projeto, devido à sua difícil legislação e, principalmente, ao facto de ser descentralizado, o que leva a que nenhuma entidade o controle.

Os *smarts contracts* são também um dos fatores importantes criados pela *blockchain*, que permitem acabar com o intermediário e reduzir os custos operacionais. Apesar de ainda estarem numa fase inicial são algo que ainda não tem consenso devido à sua complexidade, seja a nível jurídico, legal, e até informático, pois não deixam de ser programados por seres humanos, pelo que se tiveram algum erro no código podem comprometer uma série de outros contratos (Trautmanm, 2016).

A possibilidade de substituir os bancos tradicionais nas transferências globais, graças à rapidez do serviço às baixas taxas de transação, são oportunidades associadas às criptomoedas. Para além disso, o facto de serem utilizadas também como investimento, bem como um meio para combater a inflação, algo que já aconteceu no passado, concretamente com a *Bitcoin*, devido à sua rendibilidade passada. De facto, a *Bitcoin* foi o melhor investimento da década passada. Por outro lado, para investidores com mais experiências, as ICO são uma excelente oportunidade de negócios, permitindo adquirir projetos a um preço baixo.

O estudo empírico deste trabalho tinha dois objetivos fundamentais: o primeiro contribuir para um maior conhecimento sobre esta nova tecnologia, que é ainda pouco investigada a nível académico; o segundo seria o de verificar se a *Bitcoin* e *Ethereum* estariam correlacionadas com o *SP500*, bem como se a emissão dos *smart contracts* tinham impacto na rendibilidade da *Ethereum*. Para tal dividiu-se o estudo em três fases distintas, que se explicam de seguida.

Na primeira fase da análise empírica, utilizando-se dados de uma amostra dos anos de 2019, 2020, 2021 e do primeiro semestre de 2022, constatou-se que existe correlação entre a *Ethereum* e a *Bitcoin*, devido à alta volatilidade das criptomoedas e ao facto de a *Bitcoin* ser a que mais influencia o desempenho do mercado, quando está em alta o restante mercado acompanha a tendência, quando o seu preço baixa, o restante mercado das criptomoedas também acompanha. Relativamente ao *SP500* como é um índice que tem mais estabilidade, demonstrou-se não ter correlação com nenhuma das criptomoedas.

Na segunda fase foram analisadas a quantidade de *smarts contracts* emitidos e como afetavam o preço de *Ethereum*. Conclui-se que quantos mais *smarts contracts* fossem emitidos, o preço da *Ethereum* descia, devido ao facto de para emitir esse contrato é necessário utilizar *gwei*. Consequentemente quantos mais contratos forem emitidos diariamente, mais necessário é gastar *gwei* para que esses contratos sejam validados rapidamente. Isto leva a uma diminuição cotação da *Ethereum*, para que não seja gasto muito dinheiro nas transações, uma vez que o *gwei* está fixado automaticamente ao ser criado o contrato. A quantidade total de *gwei* por *smart contract* está previamente definido, não podendo ser alterado, o que varia é sim o preço que cada utilizador está disposto a pagar para que esse contrato seja emitido com rapidez, se houver um congestionamento da rede, o valor do *gwei* será elevado.

Por fim na terceira e última fase, analisou-se a variação percentual do preço médio das três amostras do estudo (*SP500*, *Bitcoin* e *Ethereum*) para os respetivos anos de 2019, 2020, 2021 e o primeiro semestre de 2022. Verificou-se que as criptomoedas tem um potencial de ganho muito superior ao do *SP500*, porém também um enorme potencial de perda, devido à sua elevada

volatilidade. Ao invés do índice *SP500*, que tem uma muito maior estabilidade, com ganhos e perdas no intervalo dos -5% a 5% normalmente.

4.1 Futuras investigações

Em investigações futuras sugere-se aprofundar a pesquisa sobre a tecnologia *blockchain*, assim como utilizar uma amostra de horizonte temporal maior para que seja estatisticamente mais significativa. Por outro lado, a analise empírica efetuada indicou um efeito correlação *Bitcoin* e *Ethereum*, pelo que seria interessante expandir esta abordagem a outras moedas de forma a verificar se a correlação se mantém.

Finalmente, seria também interessante complementar este trabalho com a pesquisa sobre outras tecnologias associadas à *blockchain*, como o *metaverso* e a *Web* 3.0, que são temáticas emergentes e intimamente relacionados com as criptomoedas. O *metaverso* seria um dos temas mais interessantes a ser aprofundados em futuras investigações, pois neste momento é uma tecnologia que está a ser testada pelas grandes empresas deste setor, como a Alphabet, Meta e Microsoft. Em consequência da pandemia do Covid-19, esta tecnologia ganhou outra notoriedade e particular relevância, devido à necessidade de as organizações manterem a comunicação e contacto entre os seus colaboradores à distância, em contexto laborar e profissional.

4.2 Limitações do estudo

As limitações encontradas para a realização da dissertação foram na revisão de literatura, devido a ser um tema ainda pouco investigado no meio académico, assim como na recolha e tratamento de dados.

O tema é ainda recente na comunidade científica, (apesar de ter mais de 15 anos) e por esse motivo, são poucas as fontes fidedignas. O tratamento de dados também é dificultado, por existirem várias plataformas que não tem o histórico do valor das criptmoedas, ao contrário do índice de *SP500*, em que é fácil encontrar informação histórica, em qualquer horizonte temporal. Por esta razão só foi possível recolher dados dos anos de 2019, 2020, 2021 e do primeiro semestre de 2022.

Também, a nível nacional há pouca investigação sobre este tema, o que reforça a relevância e pertinência desta dissertação, pelo que a pesquisa bibliográfica efetuada, baseou-se, essencialmente, em artigos e investigações internacionais.

5. Bibliografia

Alisson, I. (2017). Consultado em 10 agosto 2022.
Disponível em Maersk and IBM want 10 million shipping containers on the global supply *blockchain* by year-end (ibtimes.co.uk)

Binance. (2022). Crypto wallet types explained. Consultado em 15 setembro 2022.
Disponível em https://academy.binance.com/pt/articles/crypto-wallet-types-explained

Binance. (2020). How to use a Bitcoin ATM. Consultado em 15 agosto 2022.
Disponível em https://academy.binance.com/pt/articles/how-to-use-a-*Bitcoin*-atm

Binance. (2020). What is Bitcoin. Consultado em 15 agosto 2022.
Disponível em https://academy.binance.com/pt/articles/what-is-*Bitcoin*

Binance (2019). What is Ethereum. Consultado em 24 agosto 2022.
Disponível em https//academy.binance.com/pt/articles/what-is-Ethereum

Binance (2020). What is Fiat Currency? Consultado em 24 agosto 2022.
Disponível em https://academy.binance.com/pt/articles/what-is-fiat-currency

Binance (2019). What is hashing? Consultado em 15 setembro 2022.
Disponível em https://academy.binance.com/pt/articles/what-is-*hash*ing

Buterin, V. (2013). A Next-generation Smart contract and Decentralized Application Platform. Consultado em 15 agosto 2022.
Disponível https://*Ethereum*.org/en/whitepaper/

Cong, L. W., & He, Z. (2018). Blockchain Disruption and Smart Contracts.
https://dx.doi.org/10.2139/ssrn.2985764

Frankenfield. J. (2022). What Is Ethereum and How Does It Work? Consultado em 17 agosto 2022.
Disponível em https://www.investopedia.com/terms/e/*Ethereum*.asp

Hayes, A. (2022). What is a blockchain? Consultado em 06 agosto 2022.
Disponível em https://www.investopedia.com/terms/b/*blockchain*.asp

Luz Vieira, J. (2020). Regulação e Criptomoedas.
https://re*Po*Sitorio.ul.pt/bitstream/10451/48058/1/ulfd146078_tese.pdf

Nabil, A. (2019) Design, implementation and analysis of keyed hash functions based on chaotic maps and neural networks.
https://hal.archives-ouvertes.fr/tel-02271074

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.? Consultado em 13 agosto 2022.
Disponível em https://*Bitcoin*.org/*Bitcoin*.pdf

Nunes, F. (2021). Bitcoin. Consultado em 03 outubro 2022.
Disponível em https://eco.sapo.pt/2021/08/29/*Bitcoin*-chega-ao-mainstream-estas-10-empresas-ja-mexem-em-criptomoedas/

Pacheco, A, V. (2018). Bitcoin (10ª ed.). Editora: Self.

Peters, G., & Panayi, E. (2015) Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart contracts on the Internet of Money.
http://dx.doi.org/10.2139/ssrn.2692487

Redação. (2020). Stablecoins: o que são, para que servem e quais as mais conhecidas? Consultado em 03 outubro 2022.
Disponível em https://exame.com/future-of-money/criptoativos/o-que-sao-*stablecoins*-e-quais-existem/

Swan, M. (2015). Blockchain: Blueprint for a New Economy (1ª ed.). Editora: Media Inc, O'Reilly.

Szabo, N. (1994). Smart contracts. Consultado em 06 outubro 2022.
Disponível:https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Santos, J. V. (2021). Regulação dos Criptoativos.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3793662

Trautman, L. (2016). Is Disruptive Blockchain Technology the Future of Financial Services? The Consumer Finance Law Quarterly Report.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786186

Ulrich, F. (2014). Bitcoin. A Moeda Na Era Digital (1ª ed.). Editora Mises.

Vieira, J.P. (2017). A História do Dinheiro.
http://www.acad-ciencias.pt/document-uploads/9307616_vieira,-joao-pedro---a-historia-do-dinheiro.pdf

Wright, A., & Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia.
http://dx.doi.org/10.2139/ssrn.2580664

Zheng, Z., Xie, S., Dai, H. N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: Challenges, advances, and platforms. Future Generation Computer Systems.
https://arxiv.org/abs/1912.10370

Zola, A. (2021). Hashing. Consultado em 03 outubro 2022.
Disponível em https://www.techtarget.com/searchdatamanagement/definition/*hash*ing