ISCTE Business School
INSTITUTO UNIVERSITÁRIO DE LISBOA

Bitcoin e *Blockchain*: uma nova classe de ativos

Sérgio Ricardo Costa Baptista

Dissertação submetida como requisito parcial para obtenção do grau de
Mestre em Finanças

Orientador: Prof. Dr. Luís Miguel da Silva Laureano
Professor Auxiliar, ISCTE Instituto Universitário de Lisboa,
Departamento de Finanças

Setembro 2019

Resumo

Com o aparecimento do *Bitcoin* surge pela primeira vez na história uma moeda totalmente digital, que é ao mesmo tempo, um sistema de pagamento descentralizado. Não existindo uma entidade central, o sistema funciona com base na verificação e consenso da comunidade, com o protocolo a ter os incentivos certos, de modo a manter-se em funcionamento sem paragens nem falhas desde a sua criação, há mais de 10 anos.

O presente estudo tem como objetivo analisar a origem do *Bitcoin* e *Blockchain*, bem como o seu contexto tecnológico, económico e legal. Identificar as características que fazem do *bitcoin* uma boa moeda e quais as suas limitações, analisando a sua natureza e funcionalidade. Também é analisado a evolução de medidas estáticas e risco dos retornos do *bitcoin*, assim como essas medidas se comparam e qual a correlação do *bitcoin* com outros ativos financeiros.

Palavras-chave: *Bitcoin*, *Blockchain*, Moedas Virtuais, Sistema de Pagamento.

Abstract

With the advent of Bitcoin, emerges for the first in history a digital currency, which is at the same time a decentralized payment system. In the absence of a central entity, the system operates on the basis of community verification and consensus, with the protocol having the right incentives to keep it running without stopping or failing since its inception over 10 years ago.

The present study aims to analyze the origin of Bitcoin and Blockchain, as well as its technological, economic and legal context. Also aims to identify the characteristics that make the bitcoin a good currency and its limitations, by analyzing its nature and functionality, and analyze the evolution of static measures and risk of bitcoin returns, how these measures compare and how bitcoin correlates with other financial assets.

Keywords: Bitcoin, Blockchain, Virtual Currencies, Payment System.

Índice Geral

Índice de Figuras

Índice de Tabelas

Glossário de termos

Neste trabalho é usada a seguinte terminologia face ao termo *Bitcoin*. Quando é utilizado em maiúsculas "*Bitcoin*" está-se a referir ao protocolo. Quando é utilizado em minúsculas "*bitcoin*" está-se a referir à moeda. A mesma nomenclatura será utilizada quando forem referenciadas outras moedas ou ativos digitais, quando aplicável.

BTC -	*bitcoin*
CBOE -	*Chicago Board Options Exchange*
CNY -	*Yuan* Chinês
ECB -	Banco Central Europeu
EUR -	Euro
FinCEN -	*Department of the Treasury - Financial Crimes Enforcement Network*
GBP -	*Libra* esterlina
IBAN -	*International Bank Account Number*
JPY -	*Iene* Japonês
KRW -	*Won* sul-coreano
NSA -	*National Security Agency*
USD -	Dólar Americano

1. Introdução

Com a crise financeira iniciada em 2007, que levou à falência do *Lehman Brothers* a 15 de setembro de 2008, surgiu uma grande desconfiança no setor financeiro, e na forma como este tinha vindo a trabalhar ao longo dos últimos anos. Esta crise também motivou que surgissem críticas às políticas monetárias seguidas pelos bancos centrais, que são responsáveis pelo controlo da moeda na maioria dos países, e que utilizam na sua maioria o dinheiro fiat[1], predominante desde a queda do padrão ouro, que teve o seu fim com a intervenção do governo de Nixon na década de 80, pondo fim ao lastro que ligava o dinheiro ao ouro durante séculos.

Com este ambiente de crise financeira, no final de 2008, no dia a 31 de outubro, surge um artigo assinado por Satoshi Nakamoto, pseudónimo de um autor ou grupo de autores desconhecidos, intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Neste artigo é explicado o funcionamento de um sistema de pagamento digital que, ao mesmo tempo, é também uma moeda, totalmente eletrónico e descentralizado, sem qualquer regulação central. O mecanismo de emissão de moeda é um algoritmo matemático construído para existir um máximo de 21 milhões de unidades, com o objetivo de criar um bem escasso, tentando replicar as características que fizeram com que o ouro fosse utilizado como dinheiro ao longo de séculos (Ulrich, 2014).

As transferências são validadas por uma rede de computadores, que verifica que a moeda digital é transferida do indivíduo A para o indivíduo B, de forma anónima e encriptada (Nakamoto, 2008). A informação das transferências é guardada em blocos de transações, de onde deriva o nome dado a esta tecnologia *blockchain*[2]. Os elementos pertencentes a essa rede de validação são conhecidos como *miners*[3], são recompensados pela função desempenhada, através da criação de nova moeda e por *comissões* pagas pelos intervenientes das transferências. O histórico das transferências é mantido público, podendo qualquer pessoa aceder e validar todo o histórico de transferências efetuadas.

[1] Dinheiro fiduciário que tem como única forma de segurança a existência de um governo ou banco central que garante o seu valor, sem qualquer ativo por trás.
[2] Cadeia de blocos.
[3] Grupo de pessoas que cede ao sistema poder computacional, para validar as transações, e que em troca são recompensados pela criação de nova moeda e comissões pagas pelos utilizadores nas transferências efetuadas.

Conforme o contexto referido, o *bitcoin* tem vindo a ganhar relevância como meio de pagamento e ativo financeiro. A sua utilização como ativo financeiro tem tido principalmente relevância para investidores que procuram diversificar os seus portefólios, com um ativo que tem uma correlação baixa e até negativa com as principais moedas internacionais (Carrick, 2016) e ativos financeiros (Wu & Pandey, 2014), e também por especuladores, dada a grande volatilidade e potencialidade de valorização que o ativo apresenta.

Outros interessados no tema são as entidades estatais e outros reguladores que, devido à recente história destes ativos, têm tido dificuldade em conseguir catalogá-los nas classes tradicionais como: moedas, ações ou mercadorias. Diferentes organizações estatais, mesmo dentro do mesmo país, classificam-nos de forma díspar, não existindo para já uma uniformização de como classificar estes ativos (Prentis, 2015).

Também o setor financeiro, pela natureza inovadora e disruptiva da tecnologia *blockchain*, ainda se encontra a calcular o impacto e a utilização que esta tecnologia poderá ter no sistema bancário. Uma das grandes evoluções que esta tecnologia traz é a de não existir necessidade de um terceiro elemento, banco ou instituição financeira, que valide as transações, sendo a mesma certificada por toda a rede, podendo, esta tecnologia ter meios para substituir a banca, que atualmente cumpre a função de intermediário confiável em transações (Nakamoto, 2008). A tecnologia de bases de dados públicas, presente no *blockchain*, poderá trazer melhores formas de liquidação e venda de instrumentos financeiros, que irá diminuir os custos administrativos e tempos de liquidação (Fundchain, 2017).

A utilização do *bitcoin* poderá dar acesso a serviços bancários e pagamentos eletrónicos às populações de países em vias de desenvolvimento, sem acesso a sistemas bancários desenvolvidos. Desta forma aumentará a segurança e comodidade dessas populações. Também a redução de custo com transferências internacionais poderá aumentar as trocas comerciais e investimento estrangeiro. Estes progressos podem levar a um maior crescimento económico nestes países (Carrick, 2016).

Da literatura existente sobre o tema, dado o surgimento muito recente da tecnologia, existe uma lacuna na abrangência dos trabalhos realizados. Os trabalhos existentes são muito focados em algum aspeto em particular, tecnológico ou financeiro, não fazendo uma abordagem abrangente sobre o tema, que tente perceber o enquadramento histórico e tecnológico que levou ao surgimento do *Bitcoin,* bem como os incentivos económicos do protocolo e a sua evolução. Neste trabalho o tema é analisado sob várias vertentes, recorrendo a uma vasta bibliografia para descrever a interação entre a tecnologia e a economia do *Bitcoin,* de forma a compreender o que torna possível o seu funcionamento sem uma entidade central.

O objetivo deste trabalho é introduzir o tema do *Bitcoin* e *blockchain*, explorando a sua origem e natureza, focando-se principalmente no *Bitcoin*. Para este estudo, começarei no por fazer um breve enquadramento histórico de como o dinheiro evoluiu ao longo dos tempos, e quais as qualidades de uma boa moeda. Esta introdução tem como intuito fazer uma comparação do *Bitcoin* com os metais preciosos, nomeadamente com o ouro, que foi historicamente utilizado como moeda e reserva de valor.

Posteriormente será aprofundado o estudo do *Bitcoin*, através de uma abrangente revisão bibliográfica. Será iniciado com a evolução tecnológica que levou a surgimento do *Bitcoin* e posteriormente será explicado como o protocolo funciona, a interação entre a economia e a tecnologia do protocolo, descrevendo os incentivos existentes para o seu correto funcionamento. Também será feito um breve enquadramento legal. Ainda serão exploradas algumas das utilizações que o bitcoin e do blockchain, com foco para as funções monetárias e como ativo financeiro. No final será descrito o total do mercado das moedas virtuais, a evolução do peso do *bitcoin* neste mercado e os seus principais concorrentes.

Seguidamente será analisado a evolução do risco associado ao preço do *bitcoin*, bem como o *bitcoin* se correlaciona com outros ativos financeiros. Para este estudo serão analisados os retornos diários do *bitcoin* e de outros ativos, sendo utilizada análise estatística e calculado o *Value at Risk* empírico dos ativos, de modo a comparar o risco do *bitcoin* com diferentes produtos financeiros. Será também calculado o coeficiente de correlação linear de *Pearson,* assim como o seu nível de significância, entre os pares de

ativos em analise, de forma a analisar o potencial de utilização do *bitcoin* como um ativo que aumenta a diversificação de uma carteira de investimentos.

Conclui-se que nestes 10 anos o *bitcoin* conseguiu aumentar o seu nível de utilização, apresentado uma capitalização bolsista e volume de transações significativo. A sua volatilidade e risco financeiro têm diminuído ao longo do tempo. Apesar deste crescimento e diminuição de risco, continua a ser significativamente mais arriscado que as classes de ativos mais "tradicionais". A sua elevada volatilidade leva a que atualmente seja difícil considerá-lo como uma moeda. Como apresenta uma correlação baixa com outros ativos financeiros, a sua utilização para aumentar a diversificação de uma carteira de investimentos deve ser ponderada.

2. Revisão Bibliográfica

Neste capítulo vamos introduzir qual a origem da moeda, começando por perceber a sua função biológica e social. Posteriormente irei definir quais as características de uma boa moeda, nos seus atributos físicos e económicos.

2.1 Origem da moeda

A origem da moeda está intrinsecamente ligada ao surgimento e evolução do próprio ser humano. O Homem moderno, cientificamente denominado *homo sapiens*[4], começou por utilizar coletáveis, objetos como colares ou machados, como facilitadores de trocas, no que podemos considerar como proto moedas, sendo utilizadas desde o período Paleolítico. A sua utilização aumenta a possibilidade de trocas comerciais, permitindo a especialização entre indivíduos e tribos. A utilização de coletáveis como meio de troca veio permitir aumentar significativamente as reservas de alimento disponíveis, bem como diminuir os conflitos entre tribos. O facto de o *homo sapiens* utilizar coletáveis como meio de troca é considerado por alguns especialistas o grande diferenciador entre a nossa espécie e o Homem de *Neandertal*[5] já extinto (Szabo, 2005b).

Em termos biológicos o dinheiro serve como forma de adiamento do altruísmo recíproco, ou seja, surgiu como uma ferramenta prática e conveniente de se poder trocar favores e bens entre indivíduos de forma imediata, sem a necessidade de controlo de quem lhe deve ou a quem se deve favores. Sendo a utilização de moeda um mecanismo muito mais prático, do que fazer este registo mentalmente. Tem também a vantagem de poder ser cobrado ou utilizado com terceiros, e não apenas entre os indivíduos envolvidos na troca inicial. Este tipo de ferramenta que denominamos de dinheiro, é apenas encontrado na espécie humana (Szabo, 2005b).

O surgimento da moeda veio resolver o dilema de apenas se poderem realizar trocas voluntárias em "*coincidence of want*"[6], situação de troca perfeita em que o

[4] Homem sábio.
[5] Subespécie do homo sapiens já extinta, designada cientificamente por *homo sapiens neanderthalensi*, a sua distribuição geográfica era na Europa e Médio Oriente.
[6] Coincidência de querer, tradução do autor.

indivíduo A quer a mercadoria produzida por B, e o indivíduo B, por sua vez, quer a mercadoria produzida por A, no exato momento em que ambos têm essas mercadorias disponíveis (Szabo, 2005b).

As primeiras moedas nascem precisamente desta necessidade de troca derivada da especialização do trabalho, aceitando-se, para possibilitar o comércio, uma mercadoria que não se precise, mas que se acredite que seja mais facilmente aceite como meio de troca numa transição futura para um bem necessário, ou seja, essa matéria é utilizada como meio de troca terciário. Quanto mais uma sociedade é avançada e com maior especialização do trabalho, mais difícil a troca direta de bens se torna, sendo o dinheiro uma tecnologia essencial ao funcionamento da sociedade (Mises, 1953).

Essas mercadorias, utilizadas como meio de troca terciário, obtém valor não só da sua utilização industrial, mas também, pela sua função monetária. Com o tempo os materiais mais líquidos e mais facilmente aceites como meio de troca acabam por ganhar a condição de dinheiro, passando a sua valorização a ser devida sobretudo da sua função monetária (Mises, 1953).

Carl Menger (1892) no seu artigo "*On the Origins of Money*" definiu como principal função do dinheiro, o facto de ser utilizado como meio corrente e universal de troca, sendo que, em cada época e região, as matérias mais facilmente vendíveis ganham a função de dinheiro. O que levou os metais preciosos, na maioria das sociedades avançadas, a assumirem a função de dinheiro é a de que entre os diferentes materiais existentes, estes são os que apresentam maior durabilidade.

Os metais preciosos sempre despertaram grande fascínio nas populações, apesar da sua escassez natural, estão bem distribuídos geograficamente, sendo fáceis de extrair e trabalhar. A sua quantidade representa apenas uma pequena fração da sua procura, com um baixo custo de transporte face ao seu valor, grande durabilidade e baixo custo de armazenamento. Estes materiais, muito antes de se tornarem meio de troca, tinham uma procura positiva e constante ao longo do tempo, que junto com os seus atributos físico-químicos formaram as condições destes se tornarem dinheiro. Pois, para qualquer indivíduo e circunstâncias, existia a perspetiva de estes poderem ser trocados a qualquer momento e por variadas mercadorias, a preços de mercado. Foi esta capacidade de tornar

os negócios mais eficazes, aliado à sua durabilidade e facilidade de preservação, que fez dos metais preciosos o meio mais utilizado de acumulação de riqueza e altamente valorizado no comércio (Menger, 1892).

Menger (1976) considera ainda que o dinheiro não é produto do acordo entre homens de negócios, nem de atos legais, mas sim, que o dinheiro é um mecanismo natural e necessário à economia humana.

O papel do governo na área monetária, iniciou-se para facilitar o fornecimento de moedas uniformes e comummente aceites, os governos realizaram o trabalho de fazer essa uniformização (Hayek, 1976). Com o tempo esse serviço foi visto como muito lucrativo, dado as populações não terem outras alternativas viáveis de dinheiro. A senhoriagem, definida como o custo de cunhar as moedas, foi amplamente utilizada, principalmente durante a idade média, para o financiamento do governo. Os governos utilizavam para cunhar as novas moedas, menor quantidade de metal, metal menos puro ou de pior qualidade, mantendo o valor nominal das moedas, conseguindo desta forma reduziam os custos de produção das novas moedas, aumentando o valor na senhoriagem (Hayek, 1976).

A influência dos governos no dinheiro em circulação, que começou apenas pela cunhagem da moeda, posteriormente elevou-se ao surgimento de novas formas de dinheiro. Esse processo de criação de novas formas de dinheiro foi iniciado com a emissão de notas de crédito estatal, que por força legal, teriam de ser aceites como dinheiro (Hayek, 1976).

Inicialmente este dinheiro tinha uma convertibilidade direta a um dinheiro *commodity*. Com o passar dos tempos, as pessoas começaram a trocar diretamente este novo dinheiro e armazenando o mesmo, não o convertendo na respetiva quantidade em dinheiro *commodity*. Culminando com o governo a acabar com a convertibilidade direita do papel dinheiro, passando o seu valor a derivar em exclusivo do seu estatuto legal (Hayek, 1976).

Para Mises (1953) existem três tipos de dinheiro, 1) *commodity*, 2) fiat e 3) crédito:

1) é um dinheiro feito por base no valor de uma matéria-prima, ouro ou prata tipicamente;
2) é um tipo de dinheiro sem qualquer valor intrínseco que tem como garantia uma fonte legal estatal;
3) é o dinheiro que tem como base uma garantia pessoal, outro tipo de dinheiro ou uma matéria-prima.

A principal diferença do dinheiro fiat face ao dinheiro *commodity* é que, no primeiro, o seu valor é derivado apenas pelo seu estatuto legal, enquanto o segundo deriva do valor da livre utilização do material utilizado na moeda (Mises, 1953).

O estudo das qualidades de uma boa moeda, bem como da sua função, é uma preocupação dos pensadores e filósofos há bastante tempo. Já na Grécia antiga, o filósofo Aristóteles (384 aC - 322 aC) na sua obra *Política* descrevia o dinheiro como a medida comum de tudo, tornando possível comparar diferentes matérias ou objetos. Afirma que tudo pode ser expresso no equivalente universal do dinheiro, explicando que o dinheiro foi introduzido para satisfazer a exigência de que todos os itens trocados devem ter um termo comum de comparação.

Aristóteles definiu na sua obra Política, que uma boa forma de dinheiro teria de ter as seguintes quatro características (Aristóteles, 1998):

1) Durável, deve ser resistente ao tempo e aos elementos. Não deve desaparecer, corroer ou mudar com o tempo;
2) Portátil, ter uma grande quantidade de 'valor' face ao seu peso e tamanho;
3) Divisível, ser relativamente fácil de separar e refazer sem afetar as suas características fundamentais;
4) Valor intrínseco, o seu valor deve ser independente de qualquer outro objeto e contido no próprio dinheiro.

As características definidas por Aristóteles, das qualidades de uma boa moeda, continuam de forma genérica a serem as mesmas consideradas hoje em dia pela generalidade da literatura. Sendo as três principais características definidas atualmente: a durabilidade, a divisibilidade, a facilidade de ser transportado e armazenado. Face às características definidas por Aristóteles, apenas o atributo de valor intrínseco não é considerado hoje em dia. Sendo que pelo critério do valor intrínseco o dinheiro fiat, o mais comummente usado hoje em dia, não preencheria todos os requisitos de uma boa moeda, pois, o seu valor é apenas fiduciário e na confiança dada à entidade que gere e emite esse dinheiro.

O dinheiro *commodity* foi ao longo da história o meio de pagamento corrente, só, recentemente, com o surgimento do papel-dinheiro, na forma de notas de crédito e posteriormente fiduciário, é que o dinheiro *commodity* foi perdendo a sua dominância. A Inglaterra foi o primeiro país a assumir o padrão ouro, em 1717, quando Isaac Newton era ministro da moeda, tendo Inglaterra permanecido neste padrão até 1914 (Ammous, 2018). Neste padrão as notas e moedas de um país tinham um câmbio fixo em ouro, o que facilitava as trocas comerciais entre países com o mesmo padrão, pois, o câmbio entre as moedas era fixo, de acordo com o valor fixo em ouro de cada moeda nacional. Este padrão foi seguido pela maioria das grandes potências mundiais, tendo terminado com a Primeira Guerra Mundial, em que os governos queriam ter maior liberdade monetária para financiarem a guerra.

O padrão ouro acabou por ser substituído pelo padrão ouro-dólar. Neste padrão os bancos centrais mantinham como reserva a moeda americana como reserva de valor ou invés de ouro. Este novo padrão teve o seu fim em 1971, quando o Presidente Americano Richard Nixon acabou com a convertibilidade entre o dólar e o ouro. A partir desta data o USD deixado de ter um valor fixo em ouro, passando a ser uma moeda puramente fiduciária. Esta medida política aplicada pelo governo americano foi seguida pelas restantes economias mundiais, tendo até hoje, dado o monopólio da gestão e geração do dinheiro aos governos e bancos centrais de cada país ou região.

Desde essa altura, o ouro perdeu quase totalmente a sua função monetária, continuando a ser utilizado como reserva de valor, principalmente em ambiente de grande volatilidade nos mercados. Os próprios bancos centrais, apesar do dinheiro por si emitido

não ter nenhuma ligação formal ao ouro, continuam a ter ouro nos seus balanços por o considerarem um bom investimento, e um meio de combateram grandes desvalorizações das moedas por si emitidas.

As economias atuais utilizam tipicamente o dinheiro fiat. O dinheiro fiat é qualquer meio legal de pagamento emitido e controlado por uma autoridade central, tipicamente um Banco Central, como o Banco Central Europeu (BCE) ou a Reserva Federal Americana (FED) que respetivamente controlam o Euro e o Dólar Americano. Estas entidades têm como objetivo manter a estabilidade monetária, pelo dinheiro por si controlados, com uma meta de inflação de 2% anuais. Para além do objetivo em relação à inflação, a FED também tem um mandato de manter a economia em pleno emprego.

O dinheiro fiat não tem nenhum valor intrínseco ou reserva de valor por trás. É utilizado devido a decreto legal, bem como na confiança que os indivíduos estão dispostos a aceitá-lo como meio de troca e por confiarem que a autoridade central emitente manterá o valor do mesmo relativamente constante. A confiança é uma condição essencial de qualquer sistema monetário. Este tipo de dinheiro é comummente designado como papel-moeda.

2.2 Função económica do dinheiro

Segundo Mishkin (2010) em economia o termo dinheiro é definido como qualquer meio que é geralmente aceite como pagamento para bens e serviços, ou liquidação de dívidas. O mesmo autor refere que *"quer o dinheiro seja conchas, rochas, ouro ou papel, ele tem três principais funções em qualquer economia"*[7]: 1) como meio de pagamento, 2) como unidade de conta e 3) como reserva de valor (Mishkin, 2010: 44).

1) Meio de pagamento: a capacidade de o dinheiro ser globalmente aceite como meio de troca em comércio de bens e serviços de uma determinada região;

[7] Tradução do autor.

2) Reserva de valor: os indivíduos estão dispostos a manter a sua riqueza acumulada em moeda acreditando que no futuro a mesma não irá sofrer grande perda de valor;
3) Unidade de conta: os bens e serviços estão cotados na unidade monetária dessa moeda.

Estas funções não têm todas a mesma importância, nem são todas conseguidas simultaneamente quando um bem começa a ser utilizado como meio de pagamento. Sendo esta a função principal do dinheiro (Ulrich, 2014), é também esta função que distingue o dinheiro dos restantes ativos (Mishkin, 2010). Segundo Hayek (1976) o termo dinheiro deveria ser utilizado como adjetivo e não como um nome. No sentido que diferentes ativos têm variáveis níveis de utilização como dinheiro, não se tratado de uma propriedade absoluta de um bem.

Em relação às restantes funções, podemos considerar que são ambas derivadas da primeira. A função de reserva de valor mais não é que a esperança que o meio de troca que estamos a utilizar hoje, também possa ser utilizado no futuro. Nas palavras do economista Fernando Ulrich sobre a função de reserva de valor "*é meramente um aspeto temporal da função primordial de meio de troca manifestando-se no tempo e no espaço*" (Ulrich, 2014: 91). Para o mesmo autor, também a função de unidade de conta, acaba por ser uma consequência da grande utilização de uma moeda como meio de pagamento. O que faz com que a maioria das mercadorias e serviços acabem por ficar cotados na unidade monetária desse meio de troca.

3 Bitcoin

Neste capítulo é explorado a origem do *Bitcoin*, bem como a sua vertente tecnológica e económica. Também é explorado as utilizações do *bitcoin* e *blockchain* como moeda e ativo financeiro, bem como outras aplicações desta tecnologia. No final deste capítulo haverá uma breve introdução às principais *altcoins*[8] e protocolos alternativos ao *Bitcoin*, bem como a evolução da dominância do *bitcoin* no mercado das moedas digitais.

3.1 Origem do *Bitcoin*

Apesar do artigo que originou esta recente revolução ser apenas de 2008, já anteriormente tinha sido referida a possibilidade do surgimento de um dinheiro digital e descentralizado no mundo da internet. Esta possibilidade surge primeiramente no artigo "*The Crypto Anarchist Manifesto*" de Timothy C. May de 1988. Neste artigo o autor explica a sua visão do que irá acontecer num mundo, com a utilização da criptografia, para criação de uma moeda privada digital, bem como contratos inteligentes e autenticação descentralizada (May, 1988). Também no final da década de 90, o economista Milton Friedman, um dos mais conceituados economistas do século XX, numa entrevista dada na *NTU Talks*[9] a 1 de março 1999, previa que com o desenvolvimento da internet, poderia surgir uma moeda digital descentralizada.

A tecnologia criptográfica já é utilizada há bastante tempo na história da humanidade. A palavra e a junção de dois termos gregos, cripto que significa codificado, e grafia que significa escrita, portanto, criptografia não é mais que uma linguagem codificada, em que apenas os utilizadores que sabem o código podem aceder à informação guardada. Apesar de ser utilizada desde a antiguidade, só com a era computacional é que a sua utilização se tornou indispensável, sendo a criptografia a base de todos os sistemas de segurança atuais, nomeadamente palavras passes de bancos ou sistemas de segurança interna nacionais.

[8] Termo utilizado para designar outras criptomoedas que não o *bitcoin*.
[9] Serie de conferências organizadas pela organização americana *National Taxpayers Union*.

A primeira proposta de criação de uma moeda digital da forma como conhecemos hoje, surge com um artigo de Dai (1998) intitulado "*b-money*", onde é explicado o funcionamento básico de uma moeda através de criptografia. No entanto, este artigo não apresentava uma solução clara para o problema do duplo gasto, possibilidade de uma pessoa fazer múltiplo uso da mesma moeda. Ou seja, se uma pessoa realizasse duas transferências em simultâneo, o dinheiro era como duplicado, tendo os dois recetores finais da moeda indicação que receberam o respetivo valor. Devido a esse facto, seria necessária uma terceira entidade centralizada para validar e certificar as transferências, de modo a evitar a duplicação dos fundos utilizados.

Posteriormente Szabo (2005a) no artigo "*Bit Gold*", defini-a um protocolo muito semelhante ao do *Bitcoin*. Este protocolo já apresentava uma estrutura de blocos para se processar e verificar o histórico de transações, e um sistema de *proof of work*[10] para validar as transferências. As transferências seriam processadas em blocos com um espaçamento de tempo entre eles. Este mecanismo veio resolver o problema do duplo gasto, pois, no final de cada bloco, cada unidade monetária teria de pertencer apenas a uma pessoa. Em caso de a mesma moeda ser transferida para duas pessoas em simultâneo, no fim do bloco apenas uma das transferências seria realizada.

O "*Bit Gold*" à semelhança do *Bitcoin*, tinha como inspiração recriar a escassez natural dos metais preciosos como o ouro, de modo a dar as mesmas características que tornaram o ouro como o principal meio de troca durante séculos. Esta proposta de protocolo nunca chegou a virar uma moeda digital, é considerada o verdadeiro antecedente do *Bitcoin*. Nick Szabo é apontado como um dos possíveis criadores do *Bitcoin*. no entanto, quando questionado se é o autor do *Bitcoin* utilizando o pseudónimo de Satoshi Nakamoto, negou ser o autor, dizendo apenas que o *Bitcoin* veio trazer para o mundo real a sua visão descrita em "*Bit Gold*".

Esta evolução culminou com o lançamento do artigo de Satoshi Nakamoto de 2008, denominado "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Onde é explicado em traços gerais o funcionamento de um sistema que se viria a tornar o *Bitcoin*.

[10] Prova de trabalho ou de esforço

3.2 Tecnologia

O *Bitcoin*, foi o culminar de muitos avanços da tecnologia computacional, nomeadamente na criptografia e em sistemas descentralizados. Só com esses avanços foi possível construir um protocolo que é uma moeda e simultaneamente funciona como um sistema de pagamento. As principais inovações que estão agrupadas no protocolo do *Bitcoin* segundo Antonopoulos (2014: 3) são:

"Uma rede peer-to-peer descentralizada (o protocolo do Bitcoin)";
"Um registo de transações público (o Blockchain)";
"Uma emissão de moeda descentralizada matematicamente e determinística (distribuição da mineração)";
"Um sistema de verificação de transações descentralizado (script de transação)" [11]

Com o agrupar destas tecnologias Nakamoto (2008) conjugou num único protocolo, um sistema de verificação descentralizado, com registo de transações público, com espaçamento no processamento da informação. Deste modo resolveu o problema da necessidade de existência de uma terceira entidade centralizada que valide as transações, tornando o *Bitcoin* um sistema de pagamento autónomo e independente.

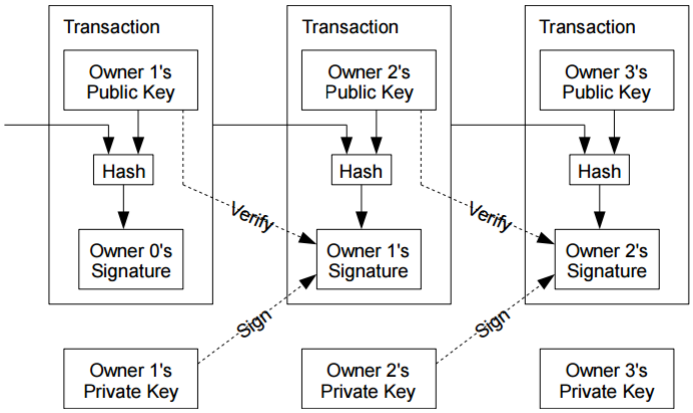
Como as transferências são realizadas através do próprio *token*[12] criado pelo sistema, o *bitcoin*, e esse *token* possui um mecanismo de emissão descentralizado, com a criação de moeda definida à partida, através de um algoritmo matemático, o que faz do *bitcoin* uma moeda com o aumento da oferta pré-estabelecido.

Conforme pode ser visualizado na Figura 1, as transações são efetuadas por um sistema de dupla assinatura digital, uma pública e outra privada. A chave pública serve para indicar qual a conta do titular dos *bitcoins*, e a chave privada como prova de propriedade. A chave privada gera a assinatura digital, e com essa assinatura o proprietário comprova que é o detentor dessa carteira de *bitcoins*. O histórico de

[11] Tradução do autor.
[12] De forma genérica o uso do termo *token* em criptomoedas refere-se a qualquer ativo digital, sendo utilizado para descrever a unidade de valor (ex. tenho X *tokens* de *Bitcoin*). O termo é sobretudo utilizado nos casos em que a função de moeda é secundária no protocolo.

transações é partilhado através de uma rede *peer-to-peer*[13], sendo verificado e chegado ao consenso usando um sistema de *proof-of-work*. Todo o histórico de transações é guardado publicamente, e com um *delay* de processamento de cada bloco de modo a evitar o *double-spending*[14] (Reid & Harrigan, 2013).

Figura 1 - Exemplo de como uma transação é efetuada através de um sistema de Blockchain.



Fonte**:** (Nakamoto, 2008: 2)

Apesar de as transferências serem realizadas de forma anónima, como o histórico de todas as transações é guardado de forma pública, consegue-se verificar através das chaves publicas, quais as transações que determinada conta efetuou. Num estudo de Andoulaki et al. (2013), chegaram à conclusão que por análise do histórico de transferências e dados públicos dos utilizadores, consegue-se chegar a cerca de 40% das identidades dos utilizadores de *bitcoin*, o que faz do sistema parcialmente anónimo. Isto deve-se a todo o histórico de transferências ser público, sendo visível quais os endereços públicos são utilizados. sabendo a quem um destes endereços pertence, facilmente podemos identificar todas as transferências realizadas por essa pessoa nesse endereço (Brito & Castillo, 2013). É aconselhável por razões de segurança e privacidade a utilização de endereços diferentes para cada operação realizada.

Na figura 2 podemos ver o exemplo de um endereço público de *bitcoin* na sua forma alfanumérica e em código QR[15]. Normalmente para se efetuar as transações entre

[13] Ponto a ponto.
[14] Duplo gasto.
[15] Sigla do inglês *Quick Response.*

contas de bitcoin é utilizado o código QR e a câmara do telemóvel, que identificando a conta de destino, seleciona-se o montante a transferir e confirma-se a transferência. Após esse processo tem que aguardar que a transação seja processada no bloco, por razões de segurança deve se aguardar que 6 blocos sejam processados, para ter certezas que a transferência não é revertida.

Figura 2 - Endereço de uma carteira de bitcoins na sua forma alfanumérica e em código QR

35GSukioZHgZu8yYjyrP3twFpLRsWkx9cU

Fonte: (Bitstamp, 2019a)

O histórico dos blocos de transferência é guardado de forma descentralizada, existindo diversos *nodes* onde essa informação fica guardada. Os *nodes* vão guardando e confirmando que os blocos de transações cumprem as regras do sistema. Um *node* é qualquer PC conectado à rede do *Bitcoin* que valida e guarda os blocos de transações efetuados. Qualquer pessoa pode ter um *node*, tendo apenas que descarregar um programa que permita validar os blocos de transferências e ter uma ligação à internet. Caso esse programa trabalhe com o ficheiro que contém o total das transferências efetuadas na rede do *Bitcoin*, estamos a falar de um *full node*[16].

Desta forma, todo o histórico fica guardado em diversos lugares. Não existindo nenhum *node* principal. O que da segurança a rede em caso de ataque de que a informação se mantém guarda e inalterada, uma vez que não existe um ponto central vulnerável. À data deste trabalho o tamanho do ficheiro onde estão gravadas todas as transações efetuadas na rede do *Bitcoin* ronda os 230 *gigabytes* (Blockchain, 2019a).

[16] *Node* completo.

As transferências são efetuadas através de uma função *hash* criptográfica SHA-256. Esta função de segurança faz parte da série SHA-2 projetada pela NSA[17]. Este protocolo de segurança é utilizado na rede do *Bitcoin* no algoritmo de *proof of work*, na criação de novas carteiras de *bitcoins*, par de chave privada e pública, e respetiva assinatura digital de validação da propriedade. A função *hash* tem por base uma determinada função y = H(x) em que é fácil de obter y dado x, mas praticamente impossível chegar a x dado y.

A função *hash* é utilizada na criação das carteiras, para gerar os pares de chaves públicas e privadas de cada utilizador. Através da chave pública não se consegue chegar à chave privada do utilizador. A chave pública serve como o número de conta ou IBAN[18], identifica quem tem a propriedade dos *bitcoins*, e em caso de transferência quem é o emitente e recetor da transação. A chave privada é o equivalente a uma *password* que serve para gerar uma assinatura digital, que comprova a propriedade de determinado endereço. É a assinatura digital que liga a chave privada à chave pública, identificando o possuidor dessa chave como legítimo proprietário do endereço. De salientar que a partir da chave privada se consegue chegar à assinatura digital, mas o contrário não é possível.

O sistema de processamento de transferências funciona através de uma rede de computadores *peer-to-peer* que, trabalhando independentemente, processam as transferências enquanto tentam resolver um problema matemático complexo. Os participantes desta rede, que cumprem a função de processar e validar as transferências são conhecidos como *miners*[19]. Os *miners* que trabalham individualmente funcionam também como *nodes*, uma vez que também guardam o histórico das transferências, mas um *node* pode não funcionar como um *miner*, caso guarde apenas as atualizações dos novos blocos, mas não processe as transferências e não tente resolver o problema matemático para criação de novos blocos. Esta opção pode-se dever a não lhes ser economicamente viável minar bitcoins, mas pretendem ter o seu próprio histórico de transações guardado.

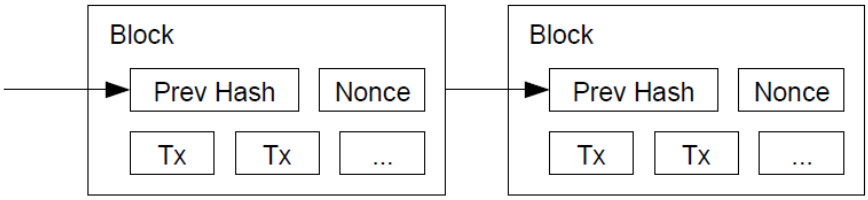
[17] Agência de Segurança Nacional Americana (em inglês: *National Security Agency*).
[18] *International Bank Account Number*.
[19] Mineiro, o termo está relacionado com a semelhança da "extração" do *bitcoin* com o ouro.

A função *hash* também é aplicada no protocolo do *Bitcoin* no *proof of work* realizado pelos *miners*, com a função de obrigar a um esforço computacional elevado e demorado, pois, apenas uma pequena alteração na função *hash* H (x+1), leva a uma grande modificação no resultado da função. Isto faz com que os *miners* sejam sempre obrigados a gastar recursos, neste caso poder computacional e eletricidade, para encontrar a solução correta. Uma vez encontrada a solução é fácil a restante comunidade verificar que o resultado chegado é o correto.

O *proof of work* é o processo de segurança utilizado pelo protocolo do *Bitcoin* em que, a cada *miner* participante é requerido resolver um difícil problema computacional, mas que após resolvido é de fácil confirmação que o resultado encontrado é o correto. O sistema está feito de modo que um *miner* com *p*% de poder de processamento da rede tenha *p*% de probabilidade de receber a recompensa associada a resolver o problema (BitFury Group, 2015). Sendo este um sistema democrático com o objetivo de chegar ao consenso de quais as transferências realizadas, cada ciclo de processamento tem direito a um voto e não o participante. Este mecanismo de segurança protege o sistema da criação de utilizadores falsos que queiram ganhar poder na rede (Böhme, Christin, Edelman, & Moore, 2015). O *proof of work* foi o meio encontrado por Nakamoto de se conseguir chegar a um consenso sem existência de uma entidade ou servidor centralizado.

Quando um *miner* chega ao resultado de um bloco, cada *node* vai confirmar que o resultado da função *hash* encontrado é o correto, e que as transferências realizadas cumprem com as normas do protocolo. A solução do bloco atual dependente sempre do seu antecedente, existindo um número designado de *nonce*, que une o valor do *hash* entre dois blocos subjacentes, conforme indicado na Figura 3. Esta ligação faz do *blockchain* uma cadeia sequencial contínua, onde não é possível fazer alterações após o bloco estar criado. Uma vez uma que uma transferência é inserida num bloco a mesma não pode ser revertida, como acontece no sistema bancário tradicional (Böhme et al., 2015). Após confirmação da validade do resultado do *hash*, é iniciado um novo bloco de transações e o *miner* que primeiro chegou ao resultado é recompensado com a criação de novos *bitcoins*, bem como pelas comissões de transação atribuídas pelos utilizadores.

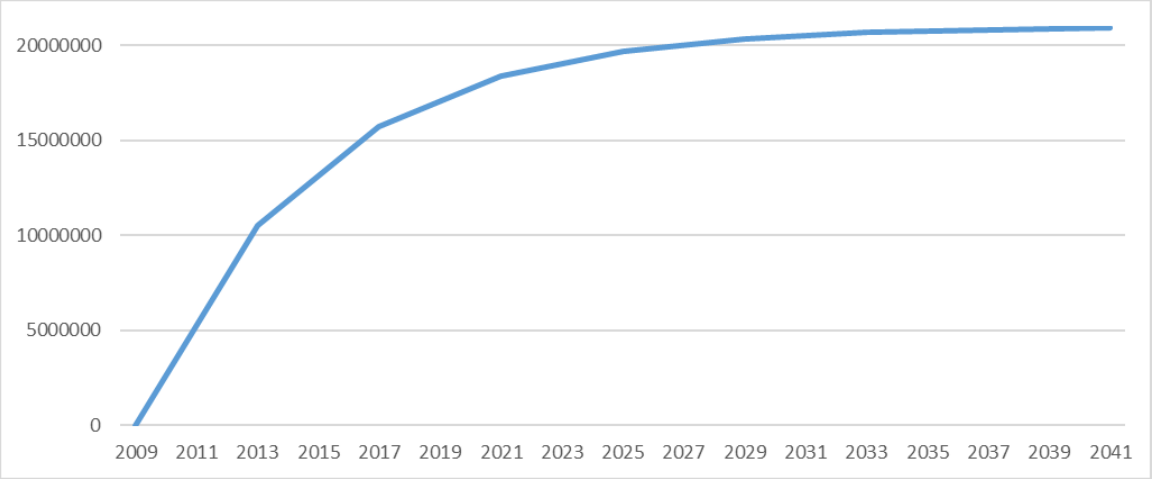
Figura 3 - Ligação entre blocos subsequentes



Fonte**:** (Nakamoto, 2008: 3)

Os blocos de transações são formados, em média, a cada 10 minutos. O *miner* que resolve o problema e fecha o bloco é atualmente recompensado pela criação de 12,5 *bitcoins*. Este mecanismo de recompensa reduz para metade a cada 210.000 blocos processados, o que acontece sensivelmente de 4 em 4 anos. A recompensa começou inicialmente por ser de 50 *bitcoins* por bloco. Na Figura 4 é ilustrada a evolução teórica do número de *bitcoins* minerados.

Figura 4 - Evolução teórica do número de bitcoins minerados



Fonte: construção pelo autor, dados (Bitcoin Wiki, 2016)

Este mecanismo de criação de nova moeda, faz com que o *bitcoin* tenha um volume máximo de moeda circulante de 21 milhões, que deverá ser atingido em 2140. A partir desse momento, não serão criados novos *bitcoin*, passando os *miners* a serem recompensados apenas pelas comissões pagas por cada transferência. Os utilizadores podem selecionar o montante da comissão a pagar. Valores de comissões mais elevados dão maior incentivo aos *miners* a processarem essa transferência de forma prioritária, face

às restantes em espera no *menpool*[20]. Atualmente o maior peso das recompensas dos *miner* continua a ser a criação de novos *bitcoins*.

A existência da *menpool* deve-se à existência de um limite ao número de transações possíveis de realizar em cada bloco, dado o tamanho máximo de um bloco ser de 1 *megabyte*. A razão do tamanho máximo do bloco deve-se a questões de ordem técnica, como a segurança da rede, e permitir a utilização do protocolo em computadores com poucos recursos, o que permite manter a descentralização do sistema (Novais, 2018).

Apesar da limitação do número máximo de *bitcoin* em circulação, este limite não cria um problema à sua utilização como moeda, uma vez que o *bitcoin* permite operar ate à oitava casa decimal 0,00000001, o que possibilita fazer-se transferências de baixo valor independentemente do preço do *bitcoin*. À unidade mínima de transação dá-se o nome de *satoshi*, um *bitcoin* vale 100 milhões de *satoshi*. O sistema para não trabalhar com casas decimais, trabalha sempre com *satoshis*, apesar de o normal ser o utilizador definir o valor a transferir em *bitcoins.*

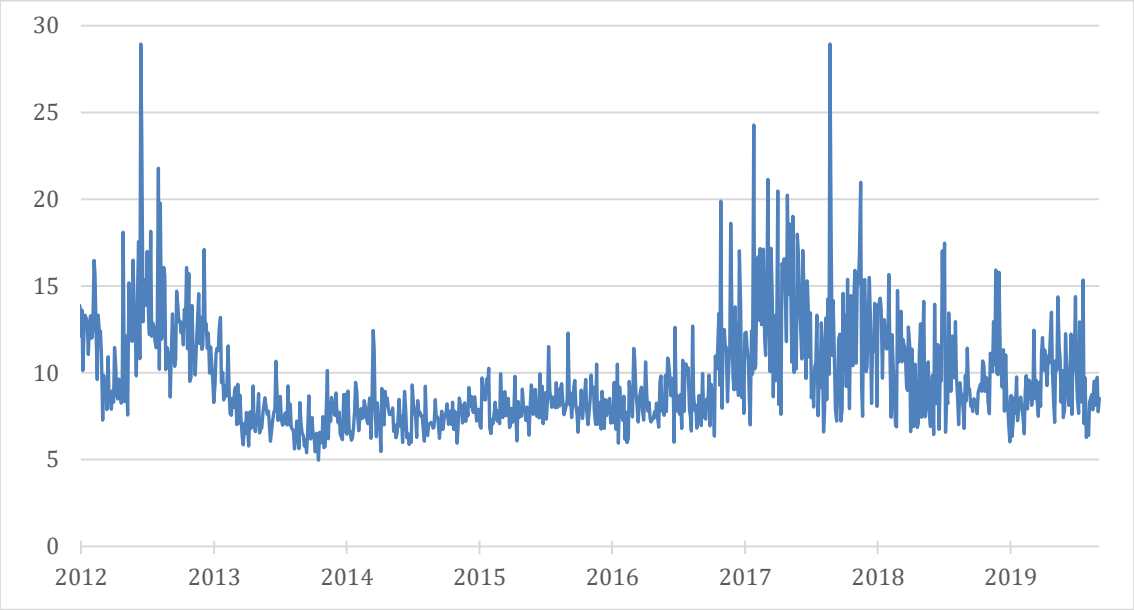
O tempo de criação de cada bloco mantém-se relativamente constante, pois, o sistema ajusta automaticamente à dificuldade do problema conforme a capacidade de processamento disponível na rede. Este ajuste do tempo é feito a partir do aumento ou diminuição da dificuldade da função *hash* do *proof-of-work.* A dificuldade é ajustada pelo sistema a cada 2016 blocos, cerca de duas semanas, de modo que o tempo de criação de cada novo bloco se mantenha por volta dos 10 minutos.

Na Figura 5 está indicado o tempo médio de criação de um novo bloco ao longo do tempo. Os picos no tempo de confirmação são devidos a momentos em que existiu uma elevada utilização do sistema, ou ocorreu uma grande queda do preço do *bitcoin* que levou muitos *miners* a abandonar a produção de *bitcoins*, pois, efetuar esse trabalho já não lhes era lucrativo, e o sistema ainda não se tinha adaptado à nova potência de computação existente. Pelo contrário, os momentos em que o tempo foi significativamente inferior aos 10 minutos, é devida à entrada de novos *miners* ser tão elevada e constante que apesar do aumento da dificuldade, o sistema não conseguia

[20] Lista de operações pendentes.

ajustar a dificuldade para o objetivo dos 10 min. Apesar de toda essa variabilidade o tempo médio desde a criação do *Bitcoin* encontra-se nos 10,3 minutos (Blockchain, 2019e).

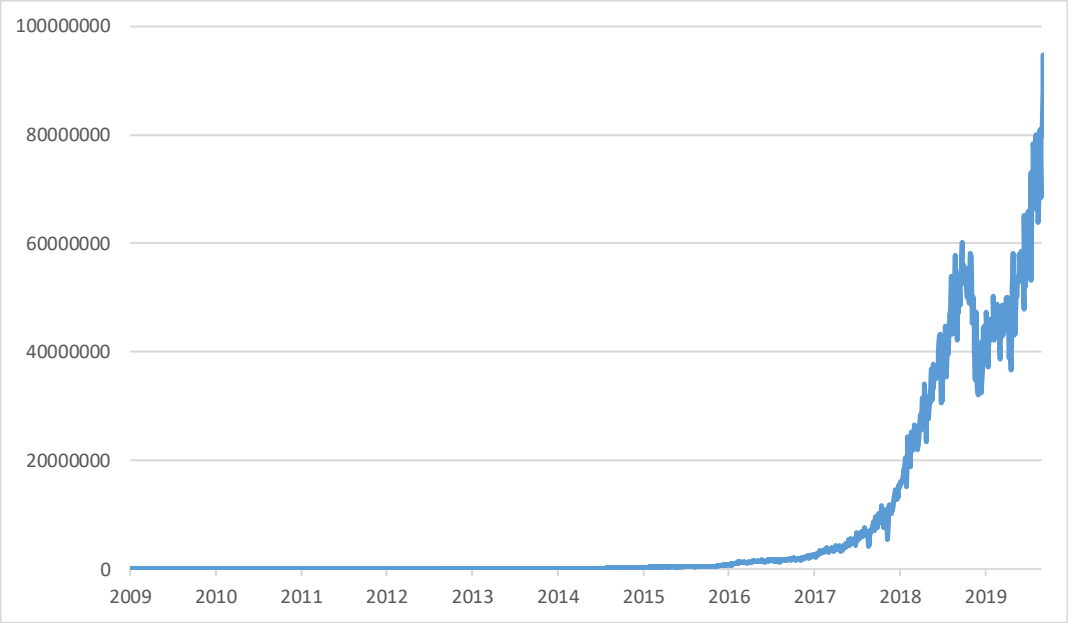
Figura 5 - Tempo médio de criação de um novo bloco em minutos



Fonte: construção do autor, dados (Blockchain, 2019e)

A evolução do poder de computação da rede figura 6, medido em *hashes* por segundo, ou seja, pelo número de resultados gerados pela função *hash* por segundo, referido como *hash rate*. Os valores têm aumentado de forma constante, apenas diminuindo quando o bitcoin sofre grandes desvalorizações de preço. Neste momento apesar de o preço do bitcoin ainda estar longe dos máximos atingidos no final de 2017, o nível de *hash rate* esta no nível mais alto de sempre. Um maior valor da *hash rate* da garantia de que o protocolo é seguro, pois, quanto maior é o *hash rate* mais difícil e caro é proceder a um ataque a rede do *Bitcoin*.

Figura 6 - Evolução da hash rate em TH/s[21]



Fonte: construção do autor, dados (Blockchain, 2019d)

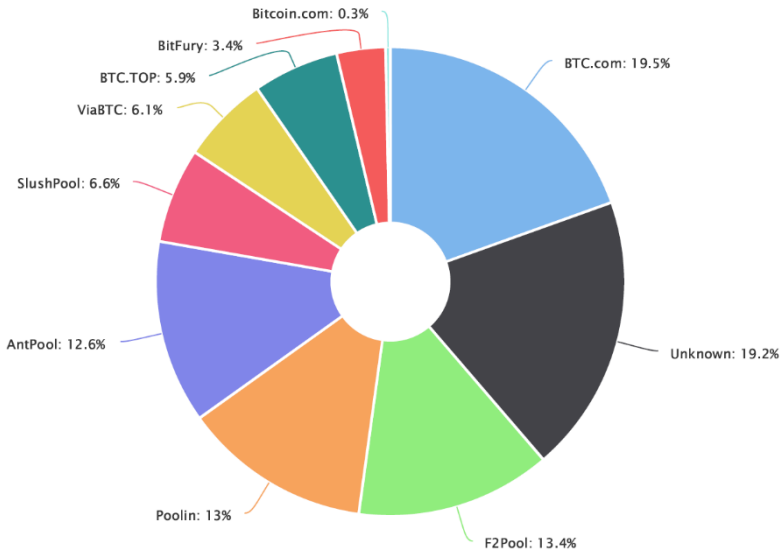
Devido a esse grande aumento do nível da *hash rate,* deforma a manter o tempo de gerar cada bloco, o nível da dificuldade de resolução do protocolo é hoje em dia tão elevada, na ordem dos 10,7 biliões de vezes mais difícil em relação à dificuldade de gerar o primeiro bloco (blockchain, 2019b). A este nível de dificuldade torna praticamente impossível uma pessoa individualmente conseguir decifrar o código para fechar o bloco de transferências, desta forma, para se minerar *bitcoin* atualmente é utilizado *hardware* especializado para realizar apenas a função de mineração, bem como fazer parte de uma *mining pool*[22] (Böhme et al., 2015).

As *mining pools* são agrupamentos de vários mineradores que juntam o seu poder de processamento para mais facilmente atingirem as recompensas de criação de novos blocos. As recompensas ganhas pela *mining pool* são depois distribuídas pelos participantes com base nos ciclos de processamento utilizados por cada elemento durante o processo. Hoje em dia as principais *mining pools* representam cerca de 80% do poder de processamento da rede, medido pela *hash rate*. Conforme indicado na Figura 7 as 4 maiores *mining pools* juntas somam mais de 50% do poder computacional. Outra grande

[21] *Tera hashes* por segundo
[22] Piscinas de mineração

vantagem de pertencer a uma *mining pool* é o aumento da previsibilidade das recompensas, uma vez que dentro da *mining pool* os resultados são distribuídos conforme os ciclos de processamento efetuados, ou invés de quem chega ao resultado do bloco.

Figura 7 - Estimativa de distribuição da hash rate entre as maiores mining pools durante 4 dias.



Fonte: Blockchain (2019b)

Apesar da sua natureza descentralizada, o *Bitcoin*, com o tempo, tem vindo a ficar mais centralizado, e esse facto deriva principalmente de duas fontes. Uma inicial, que deriva dos *core developer*, grupo dos principais programadores responsáveis pelas atualizações no protocolo, as atualizações propostas por este grupo têm de ser aceites pela restante comunidade, terem privilégios que o utilizador comum não tem. A segunda, devido à evolução do sistema e aumento da dificuldade de minar *bitcoins*, levou a que a maioria do poder computacional esteja concentrado em *mining pools*, tendo os gestores dessas *mining pools* grande poder de decisão na evolução futura do protocolo (Gervais, Karame, Capkun, & Capkun, 2014).

Um dos problemas que deriva da existência de muito poder computacional concentrado num único agente ou grupo, é a possibilidade de um ataque ao sistema conhecido como "ataque dos 51%". Nas circunstâncias em que um grupo mal-intencionado consegue ter acesso a mais de 51% do poder computacional da rede, pode selecionar a forma como os blocos serão guardados, podendo realizar transferências

maliciosas. Este ataque nunca foi realizado na rede do *bitcoin* devido ao grande custo monetário, em equipamento e em energia, necessário para se conseguir atingir a percentagem de 51% do poder computacional.

Quanto maior o *hash rate* maior é o custo de atacar a rede. Caso um ataque a rede aconteça, o grupo minoritário de *miner* e *nodes* honestos passaria a estar isolado do *blockchain* feito pela maioria maliciosa. Não validando o incumprimento das regras e criando um novo *blockchain*, fazendo com que o benefício do ataque fosse pouco significativo. Uma vez que na cadeia atacada o preço do *bitcoin* iria cair em consequência da falta de confiança no sistema por este ser controlado por um grupo malicioso.

Em certas ocasiões, algumas *mining polls* conseguiram atingir um valor próximo dos 51% do poder computacional presente na rede, nesses momentos as *miining polls* para manterem a confiança no sistema, deixaram de aceitar entrada de novos participantes até à sua percentagem de *hash rate* diminuir. Hoje em dia esta situação é mais difícil de ocorrer, uma vez que a percentagem de poder computacional nas *mining polls* estar melhor distribuída, sendo que as maiores *mining polls* individualmente têm menos de 20% de *hash rate*.

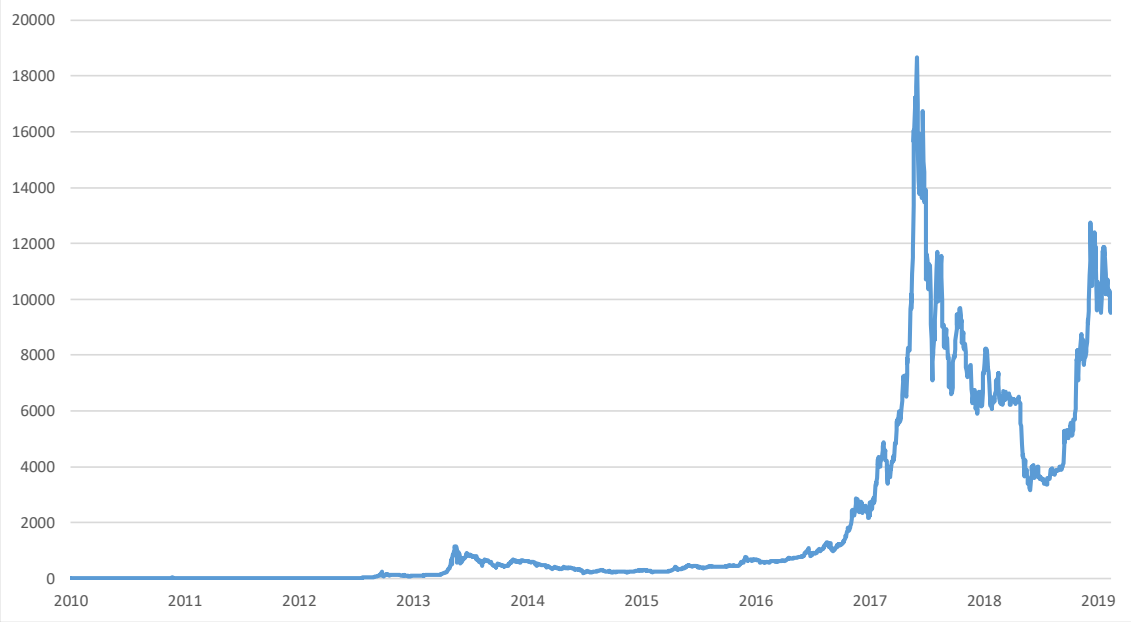
3.3 Economia do Bitcoin

A primeira moeda a surgir desta tecnologia foi o *bitcoin*, com a criação do bloco original em 2 de janeiro de 2009, quando foram emitidos os 50 primeiros *bitcoins*. Desde a sua criação que tem ganho relevância e dimensão no mercado, com uma capitalização bolsista a 4 de setembro 2019 de 187 mil milhões de dólares com um total de *bitcoins* em circulação de 17.915.112, à cotação de 10.442,12 dólares por *bitcoin* (Coinmarketcap, 2019a).

A primeira compra realizada utilizando *bitcoin* foi em 22 de maio de 2010, por Laszlo Hanyecz um programador informático da Florida que adquiriu duas pizas pelo preço de 10.000 *bitcoins* (à data da realização deste estudo essa transferência estaria avaliada em cerca de 104 milhões de dólares).

Desde esta primeira compra muitas mudanças ocorreram. Atualmente o *bitcoin* é aceite como meio de pagamento por grandes empresas como a *Microsoft* ou a *Dell*, existindo diversas casas de câmbio que fazem a conversão entre *bitcoins* e as mais diferentes moedas, sendo as principais moedas transacionadas o USD, EUR ou JPY. O CNI era a moeda mais transacionada até o governo chinês ter proibido os bancos e outras empresas financeiras de transacionar *bitcoin*, tendo posteriormente fechado as casas de câmbio locais (Ponsford, 2015).

Figura 8 - Evolução do preço do bitcoin



Fonte: construção do autor, dados obtidos através da plataforma *Bloomberg*.

O preço do *bitcoin*, ao longo da sua curta história, tem sido especialmente volátil. Começando por não ter qualquer valor quando iniciou em 2009, atingindo o seu máximo histórico perto dos 20.000 USD no final de 2017. Na Figura 8 pode-se verificar a evolução do preço do *bitcoin* ao longo do tempo. Desde 2012 os preços caíram mais de 30%, considerado um *crash* na maioria dos ativos financeiros, em 13 ocasiões conforme indicado na Tabela 1.

A queda maior e mais longa, ocorreu entre 30/11/2013 a 14/01/2015. Após uma grande escalada de preços até aos 1.163 USD, dá-se a queda da casa de câmbio *Mt. Gox*[23]

[23] https://www.mtgox.com/

que representava na altura cerca de 70% do volume de transações. A *Mt. Gox* sofreu um ataque informático onde foram roubados 850.000 *bitcoins,* que representavam 450 mil milhões de USD ao câmbio do momento do ataque. Este ataque levou a uma grade queda na confiança no sistema do *Bitcoin,* que fez o preço a depreciar até aos 152 USD.

Um grupo de investigadores considerou que a subida que levou aos máximos de 30 de novembro 2013, em que no espaço de 2 meses o preço do *bitcoin* subiu dos 150 USD até aos 1.163 USD, está fortemente correlacionada com transações suspeitas feitas através da plataforma da *Mt. Gox* (Gandal, Hamrick, Moore, & Oberman, 2018).

Tabela 1 - Quedas no preço do bitcoin superiores a 30% desde 2012

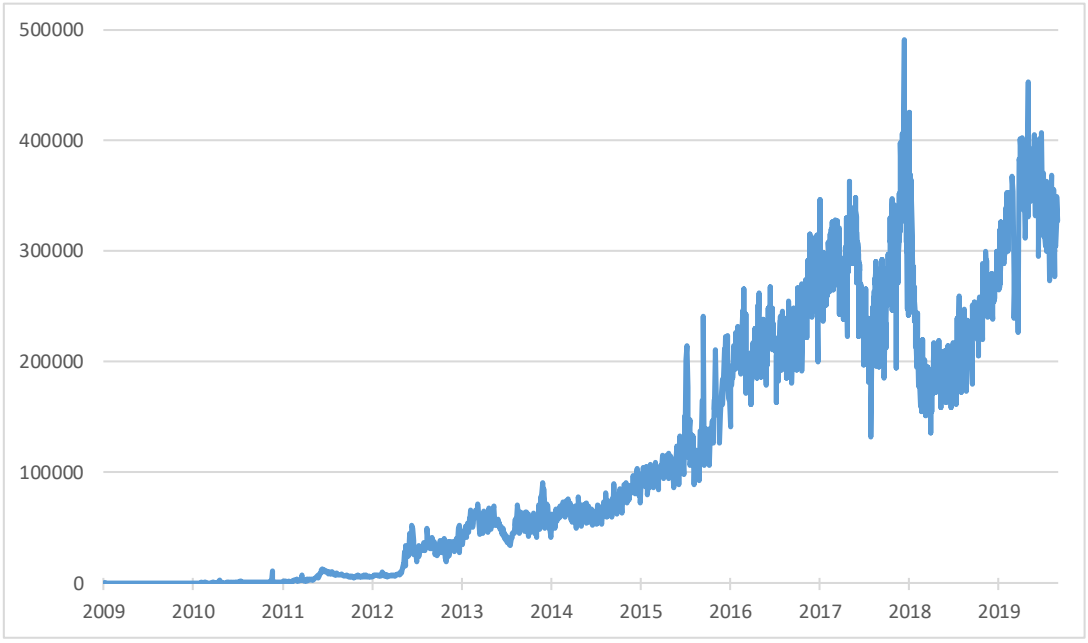
Inicio	Fim	Dias	Máximo (USD)	Mínimo (USD)	% de queda
12/01/2012	27/01/2012	16	7,38	3,80	-49%
17/08/2012	19/08/2012	3	16,41	7,10	-57%
06/03/2013	07/03/2013	2	49,17	33,00	-33%
21/03/2013	23/03/2013	3	76,91	50,09	-35%
10/04/2013	12/04/2013	3	259,34	45,00	-83%
19/11/2013	19/11/2013	1	755,00	378,00	-50%
30/11/2013	14/01/2015	411	1 163,00	152,40	-87%
10/03/2017	25/03/2017	16	1 350,00	891,33	-34%
25/05/2017	27/05/2017	3	2 760,10	1 850,00	-33%
12/06/2017	16/07/2017	35	2 980,00	1 830,00	-39%
02/09/2017	15/09/2017	14	4 979,90	2 972,01	-40%
08/11/2017	12/11/2017	5	7 888,00	5 555,55	-30%
17/12/2017	15/12/2018	364	19 666,00	3 122,28	-84%

Fonte: construção do autor, dados (Portaldobitcoin, 2019) (Bitstamp, 2019b).

Desde os máximos de dezembro de 2017, até ao mínimo da correção que foi alcançado em dezembro de 2018, o *bitcoin* desvalorizou 84%, fazendo desta queda mais recente a 2º mais longa e também a 2º maior em percentagem de desvalorização. Num estudo em que é desenvolvido um modelo de previsão de bolhas para moedas virtuais, onde eram analisados dados até 31/12/2017, indicava existência de altos indícios de uma bolha no preço do *bitcoin* (Fry, 2018).

À data deste trabalho são transacionadas através da rede do *bitcoin* cerca de 300 mil transferências diárias. Na Figura 8 está indicada a evolução no número de transações diárias. O valor veio aumentando constantemente ao longo do tempo, existindo momentos de grande subida do número de transações quando ocorrem grandes valorizações do preço do *bitcoin*, e contrações nas alturas de grandes desvalorizações do preço.

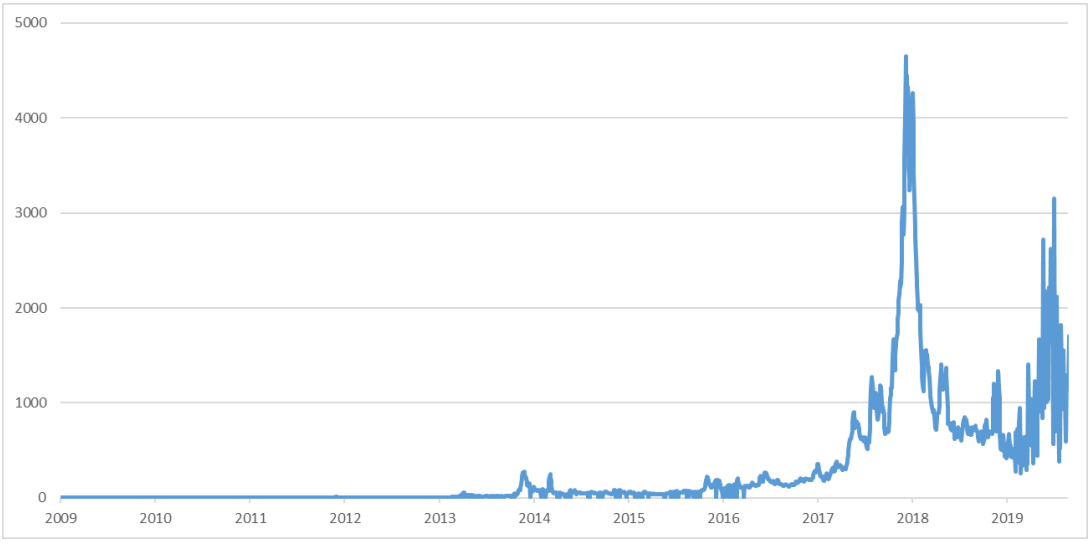
Figura 9 - Número de transações diárias



Fonte: construção do autor, dados (blockchain, 2019a)

Os valores diários transacionados na rede são de cerca de 1.000 milhões USD. Na Figura 9 podemos ver a evolução dos valores diários transacionados em milhões de dólares. É observável a existência de um grande pico no valor de transferências diárias, na ordem dos 4.500 milhões USD diários, aquando dos máximos históricos de dezembro de 2017.

Figura 10 - Estimativa do volume de transações diárias em milhões de dólares



Fonte: construção do autor, dados (Blockchain, 2019c)

Os valores apresentados nas Figuras 8 e 9 estão apenas contabilizam as transferências que são processadas via *blockchain*. A maioria das compras e vendas de *bitcoin* realizadas nas casas de cambio não são processadas no bloco de transações, bem como as transferências realizadas na *lightning network*[24]. Pelo que os valores totais de transferências diárias utilizado *bitcoin* serão significativamente superiores.

As principais casas de cambio em relação ao volume de transações efetuadas em *bitcoin* nos últimos 6 meses são a GDAZ, Bitfinex e Bitstamp, conforme indicado na Tabela 2. As casas de cambio de *bitcoin* têm normalmente mais que um par de moedas disponíveis, sendo que algumas permitem a troca direta de *bitcoins* com outras moedas digitais.

Tabela 2 - Maiores casas de cambio em volume de bitcoins transacionado durante os últimos 6 meses

Nome	Moeda	Volume (em BTC)	Spread	Trades/min
Bitfinex	USD	4 427 995	0,00%	36,25
GDAX	USD	1 678 253	0,00%	41,36
Bitstamp	USD	1 356 655	0,05%	13,41
bitFlyer	JPY	1 333 224	0,04%	33,42
Bit-x	EUR	1 240 078	1,67%	2,12
Bit-x	USD	962 612	0,02%	2,12
Kraken	EUR	890 776	1,42%	13,97
Kraken	USD	813 514	0,03%	8,05
HitBTC	USD	769 770	0,05%	7,49
itBit	USD	712 785	0,05%	3,23

Fonte: construção do autor, dados (data.bitcoinity.org, 2019)

Na fase inicial de desenvolvimento do *bitcoin,* o maior incentivo à sua utilização foi a capacidade de fazer pagamentos de forma anónima e sem mecanismos de controlo de capitais. A sua utilização inicial era sobretudo devido a atividades ilícitas como compra de bens ilegais (Böhme et al., 2015), nomeadamente através da plataforma *Silk Road*, um *site* de venda ilegal de drogas e outros materiais ilícitos, que aceitava apenas pagamentos em *bitcoin*. É estimado que mais de metade da utilização inicial de *bitcoin* fosse feita através desta plataforma (Yermack, 2013).

[24] Em português "rede relâmpago", é uma tecnologia que permite transações instantâneas e micropagamentos a custos baixos, utilizando a linguagem do *bitcoin*, sendo as transferências realizadas em múltiplos canais de pagamento independentes, não sendo as transações processadas no *blockchain*.

Num estudo realizado em 2015, onde eram analisadas as pesquisas efetuadas no *Google* sobre *Bitcoin*, com o objetivo de se perceber quais eram as principais características dos utilizadores de *bitcoin*, foram definidas 4 categorias de utilizadores: entusiastas de programação informática, especuladores financeiros, libertários e utilização para fins ilícitos. Os investigadores encontraram evidencias elevadas de utilização por parte dos grupos entusiastas de programação informática e utilização para fins ilícitos. Para os outros dois grupos as evidências de utilização encontradas foram fracas (Yelowitz & Wilson, 2015).

Dada a natureza do ativo, não se consegue explicar a evolução do preço com as teorias económicas tradicionais, tais como a evolução dos cash-flows futuros, paridade do poder de compra ou de taxas de juro. Não esta associado ao *bitcoin* nenhum pagamento de dividendos, PIB ou taxas de juro diretoras. Em geral, as moedas digitais podem ser consideradas *commodities* digitais, sendo os seus preços definidos pela lei da oferta e da procura (Kristoufek, 2013).

Em relação à eficiência do mercado no *bitcoin*, que pela teoria económica, para cada bem deverá existir apenas um preço de compra, não existindo oportunidades de arbitragem. No caso do *bitcoin* existem possibilidades de arbitragem, pelo menos teóricas, ou seja, comprar *bitcoin* numa plataforma em que o preço esteja mais baixo e vender em outra que o preço seja mais elevado, conseguindo assim um ganho sem risco, existindo cotações de preço de *bitcoin* diferentes em cada uma das casas de cambio existentes. A questão é se é lucrativo aplicar estratégias de arbitragem, considerando a existência de custos de negociação, o tempo necessário a confirmar a compra numa plataforma, transferência para outra e posterior venda dos *bitcoins*, que poderá demorar 30 ou mais minutos, existir liquidez necessária nas duas plataformas para se consumar as transações, e por último o grande capital necessário para esta estratégia tenha alguma viabilidade (Gangwal, 2016).

Apesar desta limitação, o mercado das moedas virtuais tem ganho eficiência e reduzindo a volatilidade, sobretudo nas moedas com maior liquides, que são também as com maior capitalização bolsista e negociadores ativos (Wei, 2018).

Todo o sistema está criado para existirem incentivos económicos para se chegar a um consenso, e ser bastante desvantajoso não seguir as regras do protocolo. Um exemplo destes incentivos é, no caso de um *miner* não cumprir as regras do sistema quando chega ao resultado do bloco e criar mais *bitcoin* para a sua recompensa do que os definidos no protocolo, neste caso, como existem erros na utilização do protocolo, os *nodes* não irão aceitar o bloco criado, podendo outro *miner* com o mesmo resultado fechar o bloco, seguindo as regras estabelecidas, ficando com a recompensa associada a criação do bloco. Nas situações em que um *miner* tenta enganar o sistema, não seguindo as regras do protocolo, acaba a perder os *bitcoins* e as comissões de transação do bloco do qual tinha chegado ao resultado. (Novais, 2018).

O sistema de incentivos económicos também é valido quando dois *miner* chegam ao resultado de um bloco ao mesmo tempo. Um acontecimento que ocorre com alguma frequência por razões de ordem técnicas, como a velocidade da rede. Nestas situações existem *nodes* que confirmam blocos de transferências diferentes, ao fim de algum tempo, a comunidade acaba toda por optar pelo bloco com mais confirmações, considerado esse o mais atualizado e seguro. A convergência para o bloco "maior" acaba com a bifurcação criada, pois, o risco de se estar a trabalhar no bloco "menor", que se pode extinguir, é muito elevado em relação ao custo de oportunidade de alcançar a recompensa de minerar no bloco principal que se manterá ativo (Novais, 2018).

A chegada ao consenso e a base de toda a estrutura do *Bitcoin*, como não existe uma entidade central que define como o protocolo deve evoluir, apenas com um largo consenso, as atualizações propostas são implementadas. A introdução de uma mudança não consensual leva a divisão do *blockchain* em dois protocolos, o que faz com que o valor de mercado seja diluído nas duas moedas que surgem dessa cisão, porque *miner* e *nodes* que trabalhem com diferentes regras, não podem operar uns com os outros. Desta forma, a introdução de uma mudança não consensual tem de ser bem ponderada por todos os intervenientes.

Ao fenómeno de separação de um *blockchain* em dois dá-se o nome de *hard fork*. Aconteceu no protocolo do *Bitcoin*, aquando a criação do *Bitcoin Cash*. Esta separação acorreu devido a um desacordo de como o *Bitcoin* devia evoluir, nesta situação, em relação ao tamanho máximo do bloco de transações. Este desconsentimento levou a

divisão do *blockchain* em dois protocolos e consequentemente em duas moedas, o *bitcoin* e o *bitcoin cash*. O histórico de transações de ambas as moedas é o mesmo até a data da separação, pois, até aquele momento eram a mesma moeda e protocolo. A partir da data de separação passaram a ter um histórico de registo diferente. Quem possuía *bitcoins* no momento da *hard fork* passou a deter igual quantidade de *bitcoin cash.*

Estas ruturas envolvem um grande risco financeiro para todos os intervenientes. Netas ocasiões onde há a divisão do *blockchain* em duas moedas diferentes, existe uma grande flutuação de preços, pois, os intervenientes e a capitalização são divididos entre as duas moedas. Existindo muitos possuidores das moedas a venderem uma delas, continuando apenas com a do protocolo no qual tem confiança, podendo levar a uma elevada perda financeira, com a escolha da moeda que não ganhar a maioria da aceitação da comunidade. No caso do *bitcoin cash* vale menos de 10% do valor do *bitcoin*. Devido a este risco, o mais comum é a existência de *soft fork,* que são atualizações ao sistema em que as alterações propostas não levam a uma divisão do *blockchain.* Estas atualizações só são implementadas após a existência de um largo consenso de toda a comunidade para evoluir de acordo com proposta apresentada.

É esta interação da tecnologia com a economia no protocolo do *Bitcoin*, que cria uma dinâmica com os incentivos certos, para que o sistema consiga evoluir e manter-se estável sem qualquer entidade de decisão centralizada. Mantendo um sistema de pagamento a trabalhar 24 horas por dia, 365 dias por ano, sem falhas e paragens há mais de 10 anos.

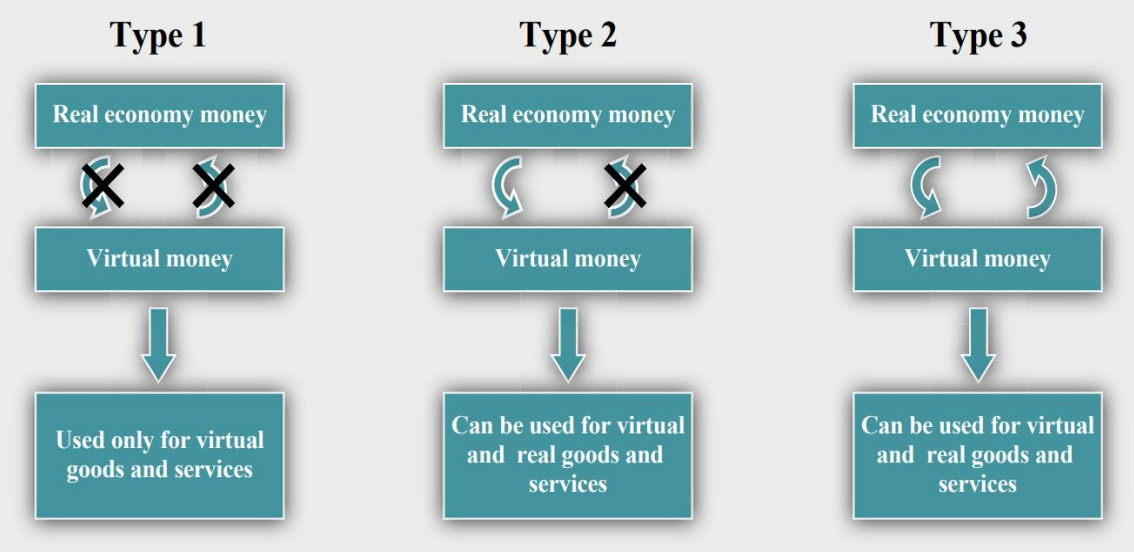
3.4 Definições legais

Devido ao *blockchain* e o *bitcoin* serem tecnologias recentes e com caraterísticas diferenciadoras, os reguladores e autoridades governamentais têm tido dificuldade em as catalogar e definir um regime jurídico para as mesmas. O facto de não ter uma entidade centrar responsável pela governação e emissão de moeda, dificulta ainda mais essa categorização pelas normas atuais.

De acordo com os regulamentos do *Department of the Treasury - Financial Crimes Enforcement Network*, a moeda é definida como "*a moeda e papel-moeda dos Estados Unidos ou de qualquer outro país que [i] seja designado como concurso legal e que [ii] circula e [iii] é habitualmente usado e aceito como meio de troca no país de emissão*"[25] (FinCEN, 2013: 1). Considerando a moeda virtual como "*um meio de troca que funciona como uma moeda em alguns ambientes, mas não tem todos os atributos das moedas reais. Em particular, a moeda virtual não tem estatuto legal em nenhuma jurisdição.*"[26] (FinCEN, 2013: 1).

O ECB considera "*Uma moeda virtual é um tipo de dinheiro digital não regulamentado que é emitido e geralmente controlado pelos seus programadores, usado e aceite entre os membros de uma comunidade virtual específica*"[27] (ECB, 2012: 5), subdividindo as moedas virtuais em 3 tipos, de acordo com a interceção destas moedas virtuais com a economia real, representação gráfica na Figura 10.

Figura 11 - Tipos de moedas virtuais pela definição do ECB



Fonte: (ECB, 2012: 15)

[25] Tradução do autor.
[26] Tradução do autor.
[27] Tradução do autor.

Tipos de moedas segundo o ECB (2012):

1) Moedas virtuais fechadas: quase não têm ligação com a economia real sendo normalmente apenas utilizadas em jogos. Os utilizadores adquirem estas moedas de acordo com o seu desempenho no jogo, sendo a utilização destas moedas limitada a compra de serviços e bens virtuais disponíveis no ambiente de jogo. Exemplo: o ouro do jogo *Word of Warcraft*[28].

2) Moedas virtuais de fluxo unidirecional: as moedas podem ser compradas usando dinheiro real a uma taxa de câmbio definida pelo proprietário do regime, não podendo ser trocada de volta para a moeda original. Podem ser utilizadas na compra de bens e serviços virtuais, algumas também permitir a compra de bens e serviços reais. Exemplo: os créditos do *Facebook*.

3) Moedas virtuais de fluxo bidirecional: a moeda pode ser comprada e vendida de acordo com a taxa de câmbio vigente. A moeda virtual é idêntica a uma moeda real, permitindo compra de bens e serviços reais e virtuais. Exemplo desta moeda: *Linden Dollars*, moeda virtual associada ao jogo *Second Life*[29].

Conforme estas definições, o *bitcoin* enquadra-se na terceira categoria, moedas virtuais de fluxo bidirecional, pois, permite a compra de bens e serviços reais e virtuais. Sendo possível a qualquer momento compra e vender *bitcoins* numa das várias casas de cambio existentes, pelos câmbios praticados pelo mercado para as diferentes moedas.

De acordo com o ECB (2012), só o 3.º tipo pode representar risco para a estabilidade financeira e credibilidade dos bancos centrais. Podendo também levantar novos desafios às autoridades públicas em relação ao branqueamento de capitais e utilizações ilícitas. À data deste relatório o ECB considerou que, apesar dos riscos mencionados, a situação não era preocupante dado a pouca liquidez que o mercado das moedas virtuais apresentava.

[28] https://worldofwarcraft.com
[29] https://secondlife.com

O ECB (2015) veio posteriormente reiterar que as moedas virtuais continuavam a não serem um risco para o sistema financeiro, uma vez que a sua utilização continuava a ser limitada. Os principais riscos destas moedas são para os próprios utilizadores, devido a grande volatilidade e risco de contraparte. O principal risco para o sistema financeiro é o possível contágio em relação a perda de confiança em meios de pagamento eletrónicos.

O Banco Popular da China, emitiu um comunicado em dezembro de 2013 em que considera as moedas digitais como uma "*commodity virtual*", tendo proibido as instituições financeiras de negociar moedas digitais, bem como trabalharem com as casas de cambio chinesas que usassem moedas digitais. Estas medidas levaram em 2014, que a maioria dos bancos chineses deixassem de fornecer serviços as bolsas de *bitcoin* (Tasca, 2015).

O Japão em abril de 2017 reconhece o *bitcoin* como meio legal de pagamento, sendo atualmente o único país a fazê-lo oficialmente, este estatuto equivale o *bitcoin* a uma moeda (FSA.JP, 2017). A lei aprovada veio também, legislar que as plataformas de negociação de *bitcoin* cumpram com normas contra a lavagem de dinheiro e KYC[30].

Alguns especialistas americanos consideram que a melhor classificação de ativos como o *bitcoin*, segundo a legislação americana, é a de *commodity*. Desta forma seria regulado pela *Council of Economic Advisers* (CEA) e qualquer produto derivado estaria sobre a alçada da U.S. *Commodity Futures Trading Commission* (CFTC) (Prentis, 2015). Este modelo facilitaria o enquadramento legal sobre a matéria.

3.5 Utilizações

Neste subcapítulo serão descritas algumas das utilizações do Bitcoin e da tecnologia blockchain, começando com a função de moeda e ativo financeira e terminando com a descrição de algumas funções alternativas desta tecnologia.

[30] Sigla do inglês "*know your customer*" em português "conhece o teu cliente", que define os procedimentos para uma empresa identificar e verificar a identidade dos seus clientes.

3.5.1 Como moeda

De acordo com as 3 funções básicas de uma moeda, podemos considerar que o *bitcoin* cumpre as funções de meio de pagamento e de reserva de valor, pese embora sua alta volatilidade pode-se considerar que não cumpre ambas as funções em toda a plenitude. Quanto a ser utilizado como unidade de conta, não o é atualmente, esse facto deve-se a não ser utilizada como moeda oficial de nenhuma nação, e a existência de poucos bens que são contabilizados diretamente em *bitcoin.* Na maioria das transações atuais para a compra de bens, o *bitcoin* é apenas utilizado como meio de troca, com os bens a serem cotados na moeda local. Também o facto de ter atualmente um grande nível de volatilidade, bastante superior as principais moedas fiat, faz com que não seja funcional a sua utilização como unidade de conta. Contudo, não existe nenhuma incapacidade formal para não desempenhar também esta função.

Na sua utilização como meio de troca, o *bitcoin* tem a vantagem de possibilitar transferências de dinheiro mais baratas, com uma data de liquidação significativamente mais curta, tratando-se um método mais eficaz e barato de meio de pagamento, sobretudo em transferências internacionais (Huang & Carlsson, 2016). É devido à sua melhor capacidade como meio de troca, que o *bitcoin* com o tempo poderá ver o seu preço valorizado, devido a sua função monetária.

Esta possível valorização derivada da sua função monetária, levará a uma maior estabilização dos preços. O que facilitaria a sua utilização como reserva de valor. Pois, com uma maior aceitação como meio de troca, levara os utilizadores a acreditar que o *bitcoin* também possa ser utilizado como meio de troca para o futuro, sem grandes desvalorizações do poder de compra.

Com as duas primeiras funções de uma boa moeda a ser cumpridas, a terceira função, de unidade de conta, surgiria naturalmente. Com o *bitcoin* a atingir um estado de grande utilização, em que os bens seriam cotados diretamente em *bitcoin* ou invés das moedas nacionais.

Ao contrário do dinheiro fiat, o *bitcoin* não é garantido ou fiduciário por nenhuma entidade central. Pode-se considerar o *bitcoin* como uma *commodity* digital, na medida

em que é um bem estandardizado, em que as suas propriedades são comuns a todas as unidades de código. Juntando o facto de o seu algoritmo simular a escassez natural de uma matéria-prima. Estas características fazem com que o *bitcoin* se assemelhe mais com o dinheiro *commodity*. No sentido em que o seu valor é intrínseco da sua livre utilização como meio de troca, derivada da confiança dada pelo protocolo, do sistema ser fiável, sendo as probabilidades de falha ou roubo das moedas guardadas reduzidas.

Também ao contrário do dinheiro fiat, a emissão de nova moeda esta predefinida matematicamente. Este facto dá confiança da não existência de desvalorizações do *bitcoin* via alteração da política monetária. Desvalorizações que acontecem com o dinheiro fiat quando os bancos centrais fazem alguma modificação, não expectável, à sua política económica e monetária.

A previsibilidade do aumento da oferta de *bitcoin* é uma das suas principais diferenças face ao ouro, pois, apesar de ambos apresentarem escassez, o ouro não apresentava um aumento da oferta conhecido, podendo aumentar fortemente com uma nova descoberta de reservas (Weber, 2016), o que podia influenciar o seu valor e função como moeda.

Após a emissão de todos os *bitcoin* disponíveis, podemos considerar que a política económica implementada no *bitcoin* como uma variante da regra "k-percentagem" proposta por Milton Friedman. Esta regra de política monetária consiste em se fixar uma taxa de crescimento de moeda, que permanecente fixa nesse valor ao longo do tempo, sendo essa taxa do conhecimento de todos os intervenientes. No caso do *bitcoin*, a partir da criação dos 21 milhões *bitcoins*, o aumento da oferta monetária é nulo. Existem outras moedas digitais que não diminuem a ofertada moeda ao longo do tempo, algumas mantêm uma taxa constante de criação de nova moeda, enquanto outras fixam a taxa de crescimento após um crescimento inicial mais elevado (Tasca, 2015).

Ter o volume de moeda fixado, e que a partir de certo ponto a oferta monetária passa a ter crescimento zero, faz do *bitcoin* uma moeda deflacionária, ou seja, com o aumento da procura de *bitcoins*, os bens tornam-se mais baratos cotados em *bitcoins*. Ao contrário do que é considerado norma pelos bancos centrais, que nos seus mandatos têm objetivos de inflação positiva fixado nos 2%, ou seja, vão aumentar ao diminuir a massa

monetária, de modo a que os preços dos produtos cotados na moeda por si gerida tenderão a subir em torno dos 2% ao ano. A defesa deste mecanismo da parte de economistas vem de considerarem que em ambiente deflacionário os consumidores tendem a preferir manter as moedas na sua posse (poupança), face a investir as mesmas em bens (consumo). O que segundo muitos economistas poderia levar a uma recessão na economia, pela alteração dos hábitos de consumo.

Ser uma moeda não inflacionável levaria que num sistema de padrão *bitcoin*, a maioria dos trabalhadores tivesse que aceitar diminuições do seu ordenado em *bitcoin* (Yermack, 2013). Apesar de essa diminuição de salário em *bitcoins*, poderia representar um aumento real do poder de compra.

O estudo realizado por Weber (2016), técnico do banco central do Canadá, sobre a possibilidade de se vir a existir um padrão *bitcoin* à semelhança do padrão ouro do passado, defende que o novo padrão teria duas principais vantagens em relação ao sistema fiat atual: 1) uma melhor previsibilidade do nível de preços, devido à taxa de criação de nova moeda ser conhecida; 2) menos custo de conversão de moeda em transações internacionais. O mesmo autor considera pouco provável o surgimento de um padrão *bitcoin*, pois, os governos e bancos centrais iram tentar evitar essa situação, sobretudo devido a duas razões: 1) para manterem a possibilidade de criarem dinheiro com custo praticamente nulo; 2) para conservarem a capacidade de controlarem o nível das taxas de juro.

Outra vantagem do *bitcoin*, derivada do facto de a sua rede ser descentraliza e de governação autónoma. Estas características tornam difícil que existam embargos ou controlos de capitais, uma vez, que para se bloquear a rede ter-se-ia que bloquear todos os elementos da mesma. Desta forma o *bitcoin* pode ser utilizado para manter o poder de compra em economias fechadas com grande inflação, como o caso da Venezuela, em que a utilização do *bitcoin* é crescente, desde o aumento da crise política e monetária.

Para habitantes e empresas presentes em mercados emergentes, como um meio de transferência ou complemento a moedas ditas tradicionais, principalmente como meio de troca em transferências internacionais, pois, em países com moedas mais “fracas” e com um sistema bancário pouco desenvolvido, os custos de transferência e cambiais podem

atingir valores superiores a 10% da transação final, tendo a mesma transferência através da plataforma de *Bitcoin*, custos bastantes inferiores, entre o 1% e os 2% (Carrick, 2016).

Podemos também considera como vantagem da utilização de *bitcoin* como meio de troca, a facilidade de utilização e sem intermediários, que poderia levar ao desenvolvimento de países em que o sistema bancário não é desenvolvido, em que a rede bancária não dispõe de uma cobertura territorial abrangente, em que os seus habitantes não têm acesso a contas bancárias ou cartões de pagamento. Para a utilização da tecnologia *Bitcoin* é apenas necessário um terminal com acesso à internet e um mecanismo de conversão do *bitcoin* na moeda local. Nestes países o uso do *bitcoin* traria maior segurança e comodidade as populações locais (Carrick, 2016).

Para os comerciantes a utilização de *bitcoin* pode ter ainda maiores vantagens, como os custos com pagamentos são inferiores aos aplicados com cartões de crédito ou débito. O tempo de liquidação ser significativamente menor, os pagamentos com cartões demoram cerca de 60 dias a serem liquidados. Também o facto de as transferências realizadas serem imutáveis, diminuiria os custos com fraudes e reversões de pagamentos. Estas vantagens fazem com que comerciantes possam apresentar preços mais competitivos aos clientes que utilizam o *bitcoin* como meio de pagamento.

Como desvantagem, devido ao protocolo ser parcialmente anónimo, a utilização do *bitcoin* pode facilitar a realização de fins ilícitos, como o branqueamento de capitais e lavagem de dinheiro, sendo que nessa matéria assemelha-se muito a utilização de "dinheiro vivo".

Outra desvantagem apontada é o facto de existir um limite de transações que podem ser executadas. Bem como o tempo de liquidação ser no mínimo de 10 minutos, tempo para processar um bloco de transferências, sendo recomendado esperar por 6 blocos para se ter certeza que a transferência não será alterada, o que demora cerca de uma hora. Esta desvantagem é mais significativa em relação à utilização do *bitcoin* como meio de pagamento do dia a dia. Os problemas de escalabilidade têm sido ultrapassados pela introdução de novas tecnologias que são aplicadas ao protocolo do *Bitcoin*, nomeadamente com a *lightning network*, que permite pagamentos instantâneos e sem o problema do número limitado de transações.

A grande volatilidade atual do *bitcoin* dificulta a sua utilização como meio de pagamento. A volatilidade no *bitcoin* é bastante mais elevada do que nas moedas fiat mais utilizadas. A grande volatilidade também dificulta a utilização como reserva de valor e unidade de conta, o que faz que nas condições atuais alguns autores não considerem o *bitcoin* como uma moeda (Baur & Dimpfl, 2017) (Gangwal & Longin, 2018).

Caso o *bitcoin* ou outras criptomoedas venham a ser comummente utilizadas como meio de pagamento, poderemos ter uma nova fase de utilização de múltiplas moedas, num regime de utilização de dinheiro fiat e moedas digitais. A utilização de várias moedas dentro do mesmo território era uma prática comum durante a idade média, onde o ouro, a prata e cobre eram simultaneamente utilizados como meio corrente de pagamento. No início do século XX era comum nos Estados Unidos a circulação simultânea de dinheiro *commodity* e fiat. Ainda hoje em dia é comum a utilização simultânea de duas moedas, em países da América Latina, com a utilização do dólar americano em paralelo com a moeda local, ou na Suíça em que a utilização do Euro em complemento ao Franco Suíço é comummente aceite (Baur, Hong, & Lee, 2018).

3.5.2 Como ativo financeiro

A utilização do bitcoin como ativo financeiro advém muito da grande valorização que o ativo apresentou desde sua criação bem como a sua grande volatilidade que dá oportunidade de negociação aos investidores. Por outro lado, o facto de ser um ativo que tem apresentado correlações baixas ou negativas com diferentes classes de ativos, leva que possa ser utilizado como um ativo que aumenta a diversificação de uma carteira.

Num dos estudos sobre o tema, em que se analisa a correlação do *bitcoin* com diversas moedas, chegou-se à conclusão que o *bitcoin* tem correlação negativa com a maioria das moedas, quer de países desenvolvidos, quer de mercados emergentes. O autor considerou o *bitcoin* como um bom ativo a ser utilizado para diversificação de risco cambial (Carrick, 2016).

Num artigo realizado por Warwick (2016), onde foi verificado a correlação do *bitcoin* com diversos ativos financeiros, tendo por base os retornos a 10 dias no período de 6/30/2013 a 7/31/2016. O autor constatou que existe uma baixa correlação com a

globalidade dos ativos analisados, variando entre -0,16 e 0,13. Concluindo que o *bitcoin* pode ser utilizado para aumentar a diversificação na maioria dos portfólios.

Em outro estudo, onde se analisa qual a correlação do *bitcoin* com o ouro, em diferentes momentos do mercado acionista. Chegaram a conclusão que o *bitcoin* tem um comportamento díspar do ouro em momentos de queda no mercado acionista. A tendência do *bitcoin* é de acompanhar o mercado acionista durante as quedas, ao contrário do ouro que demonstra correlação negativa nessas circunstâncias. Desta forma a conclusão do estudo é de que o *bitcoin* não se comporta como um ativo de *hedged*, mas apenas como um elemento de aumento da diversificação (Klein, Pham Thu, & Walther, 2018).

Numa análise a utilização do *bitcoin*, onde se agrupa os utilizadores por categorias de acordo com as transferências realizadas, em relação ao número e montantes. Os investigadores chegaram a conclusão que a utilização de *bitcoin* tem aumentado sobretudo devido ao crescimento de utilizadores que o utilizam como ativo financeiro (Baur et al., 2018). O mesmo estudo também chegou a conclusão que o *bitcoin* apresenta caraterísticas de diversificação em momentos normais e de turbulência nos mercados.

Em outro estudo onde se pretendia mediar a capacidade de diversificação do *bitcoin* numa carteira. Chegaram a conclusão que uma pequena percentagem de *bitcoin* reduzia a volatilidade da carteira. Apresentando melhores resultados quando junto numa carteira diversificada, que também detinha outros ativos considerados como *hedging*, como ouro, petróleo ou ações de mercados emergentes (Guesmi, Saadi, Abid, & Ftiti, 2018).

De acordo com Wu & Pandey (2014) os investidores individuais beneficiariam em terem uma pequena quantidade de *bitcoin* em carteira. O estudo tem por base o investimento num portefólio devidamente diversificado, nestas condições a carteira de variância mínima detinha 0,57% do seu valor investido em *bitcoin.*

Em relação à diversificação entre moedas virtuais, um grupo de investigadores chegou a conclusão que deter apenas *bitcoin* em carteira, é no mínimo igualmente tão bom, como ter um portefólio diversificado com as outras principais moedas virtuais (Platanakis, Sutcliffe, & Urquhart, 2018).

3.5.3 Utilizações alternativas

Dada a sua tecnologia de bases de dados públicas e descentralizadas, podem surgir muitas utilizações do *Bitcoin* ou nestes casos talvez mais especificamente do *blockchain*, que as funções mais diretas, monetárias e financeiras, já mencionadas.

Uma dessas utilizações são os chamados *smart contracts*[31],onde se pode associar todo a espécie de acordos entre dois ou mais intervenientes. Estes contratos podem representar propriedades físicas ou digitais. A partir desta tecnologia podem aparecer, por exemplo, contratos de empréstimo ou aluguer de carros automáticos, que cancelem automaticamente quando o utilizador deixa de pagar a prestação, perdendo a sua chave digital de aceso a viatura (Catalini & Gans, 2016).

A capacidade de a tecnologia *blockchain* de rápida liquidação e o facto de o histórico de transações ser público, pode facilitar os gestores de fundos a distribuir de maneira mais eficiente os seus produtos. O uso desta tecnologia pode reduzir os custos administrativos com servidores centrais e liquidações (Huang & Carlsson, 2016). Em Portugal a Associação Portuguesa de Fundos de Investimento, Pensões e Patrimónios (APFIPP) lançou uma plataforma de distribuição de fundos de investimento com base em tecnologia *blockchain,* que se encontra em fase de teste.

Ao nível Europeu existem alguns projetos do mesmo género, sendo o de maior notoriedade o *FundChain*[32]. Uma iniciativa luxemburguesa que conta com a parceria de empresas importantes da indústria dos fundos de investimento, como a *Pictet*[33] e o *BNP Paribas*[34]. O objetivo desta plataforma é avaliar a viabilidade de utilização de sistema de venda e liquidação de fundos de investimento, através de uma rede privada *blockchain*, tendo por base o protocolo do *Ethereum*. Esta plataforma tem como objetivo ser utilizada como meio de distribuição, custódia e liquidação de fundos de investimento, permitindo uma diminuição de custos e do tempo de liquidação dos ativos (Fundchain, 2017).

[31] Contratos inteligentes.
[32] http://fundchain.lu
[33] Banco privado suíço, mas conhecido pela gestão de investimentos https://www.group.pictet.
[34] Um dos maiores bancos europeus https://group.bnpparibas.

Também da existência de contratos inteligentes e de histórico público, podem surgir plataformas de serviços ou distribuição de conteúdos descentralizados. A semelhança das plataformas já existentes (ex. *Uber, Airbnb, Youtube*), mas sem as empresas intermediárias centralizadas. A criação destas plataformas através de protocolos de *blockchain* traria custos mais baixos e maior transparência aos consumidores (Catalini & Gans, 2016).

3.6 *Altcoins*

Altcoin é o termo utilizado para referir outras moedas virtuais ou protocolos que não o *Bitcoin*. À data deste trabalho existiam mais de 2085 moedas virtuais, com uma capitalização bolsista total de 203 mil milhões USD. As 10 maiores moedas em capitalização bolsista representam 85% do mercado. Na Tabela 3 estão indicados os valores de mercado e a capitalização bolsista das 10 primeiras moedas digitais em capitalização bolsista.

Tabela 3 - Capitalização bolsista das principais moedas virtuais.

Moeda	Preço	# moeda emitida*	Capitalização Bolsista
Bitcoin	$10 367,49	17 925 157	$185 838 885 790
Ethereum	$182,68	107 669 839	$19 669 126 256
XRP**	$0,26	42 984 595 777	$11 266 692 399
Bitcoin Cash	$307,16	17 993 562	$5 526 902 640
Litecoin	$69,98	63 218 189	$4 424 008 840
Terher**	$1,00	4 084 519 730	$4 084 519 730
EOS**	$3,87	931 564 886	$3 605 156 107
Binance Coin**	$22,34	155 541 838	$3 474 804 655
Bitcoin SV	$133,29	17 854 791	$2 379 865 114
Monero	$76,65	17 200 197	$1 318 395 130

*Na respetiva unidade monetaria de cada moeda

**Moedas não mineráveis

Fonte: Construção do autor, dados (Coinmarketcap, 2019a)

O termo *altcoin* significa moeda alternativa. O seu significado deriva do *bitcoin* ter sido a primeira moeda virtual a surgir, bem como pelo grande domínio que o *bitcoin* tem no mercado das moedas virtuais. Muitas destas moedas não pretendem ter como uso final o de meio de pagamento, mas são apenas um *token* para garantir que existem

incentivos para os *miner* mantenham o funcionamento do sistema para o verdadeiro propósito do protocolo. Por exemplo, o *Ethereum* tem como objetivo ser uma plataforma onde se celebram contratos inteligentes.

O *bitcoin* ao longo dos anos tem perdido parte da sua dominância no mercado das moedas virtuais. Historicamente tem uma percentagem do mercado muito elevada, quase sempre superior aos 80%. O período de maior dominância durou até ao início de 2017, quando os seus concorrentes mais diretos, *ripple* e *ethereum,* começaram a ganhar maior relevância e capitalização. Parte desse fenómeno deveu-se a especulação da existência de uma *hard fork* no *bitcoin*, que pressionou o preço da moeda. Essa *hard fork* veio a ocorrer em 1 de agosto de 2017, quando deu início a circulação do *bitcoin cash,* a data deste trabalho a 4 maior moeda virtual em capitalização bolsista. Neste período de controvérsia e incerteza a dominância do *bitcoin* desceu abaixo dos 40% do total do mercado.

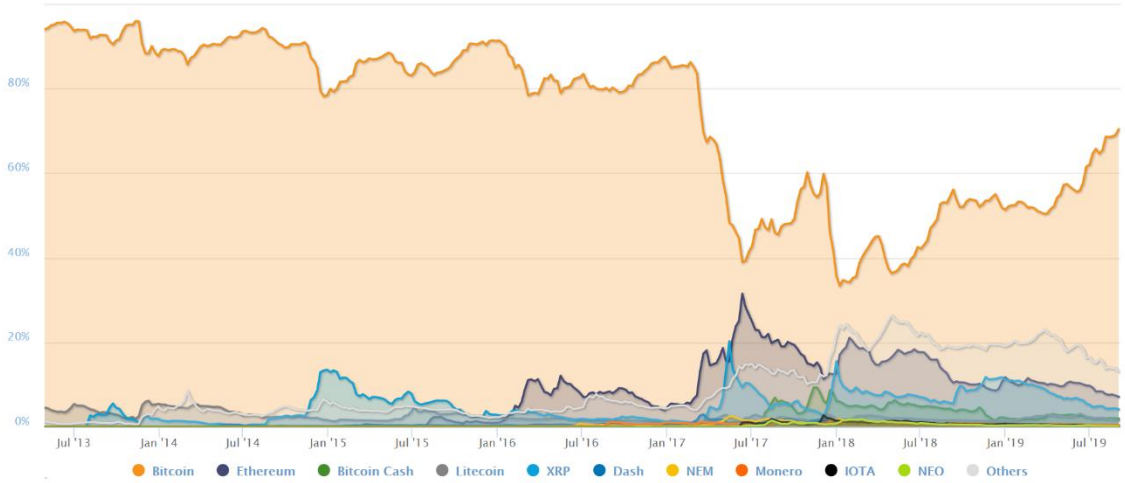
Após consumada a *hard fork,* a dominância cresceu novamente, ficando acima dos 60%, quando o preço de *bitcoin* subiu até o seu máximo histórico em dezembro de 2017. Após esse período, voltou a cair na sequência da correção dos máximos, tendo atingido o seu mínimo histórico de dominância nos 32% em meados de janeiro de 2018. Desta vez, esta diminuição foi sobretudo devido ao aumento do número e valor de novas moedas digitais, muito devido a grande quantidade de ICO[35].

As ICO são vendas iniciais de uma nova moeda, semelhantes às entradas iniciais em bolsa. Servem para angariarem dinheiro para o desenvolvimento do projeto de criação de uma moeda ou protocolo. Muitos destes projetos nesta fase não passavam de um esboço ou ideia de utilização.

Desde esse mínimo, voltou a ganhar percentagem da capitalização bolsista, tendo o valor de 71% a 5 de setembro 2019. A evolução da dominância do *bitcoin* no mercado das moedas virtuais pode ser visualizada na Figura 12.

[35] Sigla do inglês *Initial Coin Offering.*

Figura 12 - Percentagem do total da capitalização bolsista das moedas virtuais



Fonte: (Coinmarketcap, 2019b)

Os principais concorrentes do *Bitcoin* são o *Ethereum* e o *Ripple*, tendo uma capitalização de 19 e 11 mil milhões USD respetivamente (Coinmarketcap, 2019a).

O *Ethereum*[36] é uma plataforma descentralizada, com o foque na criação de *smart contrats*. No protocolo do *Ethereum* existe um valor a pagar por cada operação, sendo que esse custo é pago com *ether*, a moeda nativa do sistema.

O *Ripple*[37] é um sistema de liquidação bruta em tempo real, que é constituído por um protocolo distributivo aberto, com um banco de dados de operações publico e uma moeda nativa o XRP. Tem das confirmações de transação mais rápida dentro do género, sendo considerada a opção de liquidação mais eficiente para fluxos interbancários. É atualmente utilizado por instituições financeiras como o *Santander* e a *American Express*.

[36] https://www.ethereum.org.
[37] https://www.ripple.com.

4. Dados

A fonte utilizada para a recolha de dados para este estudo foi a plataforma Bloomberg.

Para a análise do *bitcoin*, considerou-se o preço de fecho do *Bitcoin Bloomberg Index* (*ticker*: XBT BGN Curncy). Foram utilizados os dados referentes ao período entre 7 de junho de 2010 e 30 de agosto de 2019, início dos dados disponível na plataforma utilizada.

Para os restantes ativos analisados no estudo, considerou-se o período de 30 de agosto de 2018 a 30 de agosto de 2019, contabilizando 1 ano de cotações e 263 observações diárias do preço de fecho.

Listagem de todos os ativos considerados na análise:

- EUR (*ticker*: EUR *curncy*);
- Ouro (*ticker*: XAU *curncy*);
- MSCI *World Index* (*ticker*: MXWO *Index*) – índice de ações mundiais;
- Euro-Bund 10-Year Futures (*ticker*: RX1 *Comdty*) – futuros de dívida alemã a 10 anos;
- CBOE *Volatility Index* (*ticker*: VIX) – é uma medida da expectativa de volatilidade do mercado de ações implícita nas opções do índice S&P 500.

Foram considerados os preços em USD para todos os ativos analisados.

5. Metodologia

O tratamento de dados deste trabalho está dividido em duas fases. Na primeira a análise incidiu apenas no ativo *bitcoin*, onde será analisada várias medidas estatísticas, para identificar como o risco associado ao preço do *bitcoin*, tem evoluído ao longo do tempo. Na segunda fase do estudo, será comparado o risco do *bitcoin* com os restantes ativos considerados. Bem como a correlação linear e o seu nível de significância entre os pares de ativos analisados.

Para a primeira fase começou-se por realizar uma uniformização dos dados e calculado o logaritmo dos preços diários do *bitcoin:*

$$R_t = Ln(P_t/P_{t-1}) \quad (1)$$

Posteriormente procedeu-se a uma análise estatística para cada um dos períodos em estudo, correspondentes a um, três e cinco anos, e desde do início de 2011. Foram desconsiderados os dados anteriores 2011, pois apresentarem grandes oscilações nos preços, alternados com momentos de variação nula. Para além do pouco volume e grande volatilidade deste período inicial da negociação do *bitcoin*, a situação é ainda agravada devido à existência de apenas 2 casas decimais nos dados disponíveis através da plataforma *Bloomberg*. A existência de apenas 2 casa decimais numa altura em que o preço do *bitcoin* estava nos poucos cêntimos, faz aumenta a variação da amostra nesse período.

A análise estatística foi realizada utilizando as ferramentas disponíveis no programa *Excel* do *Microsoft Office,* para cálculo de medidas de estatística descritiva para os vários horizontes temporais em estudo. Estes cálculos têm o intuito de ver como estas medidas evoluíram ao longo dos diferentes horizontes temporais em análise. As medidas estatísticas calculadas foram: média; máximo; mínimo; variância; desvio padrão; simetria e o excesso de curtose.

Ainda nesta fase, para além da análise estatística, foi também realizado o cálculo do *Value At Risk* (VaR) dos retornos do *bitcoin* para os mesmos períodos. O VaR é uma

medida estatística que avalia o nível de perda máximo expectável de um ativo financeiro ou carteira, para um determinado horizonte temporal e probabilidade de ocorrência de perda. É uma medida utilizada para gestão do risco expectável de um ativo ou carteira de investimento, bem como para definir rácios mínimos de capital. Uma vantagem do VaR em comparação a medidas de risco tradicional, como a volatilidade, é que o VaR tem em conta apenas as probabilidades de perda.

Neste estudo foi calculado o VaR empírico, utilizando a distribuição das observações históricas. Para tal foram utilizados os logaritmos dos retornos diários do ativo, tendo sido ordenados em ordem crescente de valorização, para cada um dos períodos em análise, de modo a identificar o valor de perda expectável do VaR para os níveis de significância de 95% e 99%. Identificando para cada período, qual o valor de perda para as ocorrências de 1% e 5% da amostra histórica.

A utilização do VaR empírico ao invés de um VaR paramétrico deve-se a distribuição histórica do *bitcoin* afastar-se significativamente da distribuição normal. O afastamento é sobretudo devido à existência de caudas longas. Desta forma a utilização do VaR empírico dá valores mais próximos da realidade do que o VaR paramétrico.

Na segunda parte da análise foram comparados os retornos do *bitcoin* com outros ativos financeiros em termos estatísticos e de VaR, para o período temporal de um ano. Foram analisadas 263 observações do preço de fecho de sessão, o que corresponde a 262 retornos diários. Para se proceder a essa análise, começou-se por uniformizar os dias das observações para cada ativo. Tendo sido aplicado para cada ativo a mesma metodologia indicada na primeira parte para o cálculo das medidas estatísticas e de VaR.

Posteriormente a essa análise inicial, foi calculado para os mesmos ativos e horizonte temporal indicado. O coeficiente de correlação linear de *Pearson* e respetiva significância estatística entre cada um dos pares de ativos analisados.

O coeficiente de correlação de *Pearson* mede o nível de correlação linear entre duas variáveis. Os valores do coeficiente podem variar entre 1 e -1. Onde o valor de1 representa uma correlação linear positiva perfeita, e o valor de -1 representa uma

correlação linear negativa perfeita. O valor de 0 significa que não existe correlação linear entre as duas variáveis.

Para o cálculo do coeficiente *Pearson* foi usada a seguinte equação:

$$\rho = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2}.\sqrt{\sum_{i=1}^{n}(y_i - \bar{y})^2}} = \frac{cov\ (X,Y)}{\sqrt{var\ (X)\ .var\ (Y)}} \quad (2)$$

Posteriormente foi calculado o nível de significância estatística do coeficiente de *Pearson* para cada par de ativos, sendo aplicado o teste estatístico:

$$t = \frac{\rho\sqrt{n - 2}}{\sqrt{1 - \rho^2}} \quad (3)$$

Com n igual ao número total de retornos diários, 262. Para analisar o valor do teste foi aplicado o teste de hipóteses:

H_0: $\rho = 0$
H_1: $\rho \neq 0$

Para cada um dos pares de variáveis foi analisado os valores críticos da distribuição t de *Student* 1,65; 1,96 e 2,58, para os valores de significância de 10%, 5% e 1% respetivamente. Os valores críticos são bilaterais, uma vez que foi considerado a hipótese alternativa como $\rho \neq 0$, podendo a correlação linear ser positiva ou negativa. Caso o modulo do valor de teste estatístico for superior ao valor critico, rejeitamos H_0, e podemos assim concluir que existe significância estatística para uma relação linear entre as variáveis.

6. Análise de resultados

Conforme indicado no capítulo 5, este estudo ira começar com a análise estatística e de VaR dos retornos do *bitcoin*, para diferentes horizontes temporais.

O preço do *bitcoin* tem sido historicamente muito volátil, com uma média de valorização bastante elevada. Significativamente superior aos ativos financeiros tradicionais, o que tem levado a que seja encarado como um investimento especulativo.

Tabela 4 - Analise estatística e VaR a diferentes horizontes temporais do bitcoin

	BTC desde 2011	**BTC 5 anos**	**BTC 3 anos**	**BTC 1 ano**
Média	0,46%	0,23%	0,36%	0,13%
Máximo	51,70%	22,32%	22,32%	22,32%
Mínimo	-60,09%	-26,10%	-26,10%	-17,53%
Desvio padrão diario	6,26%	4,40%	4,84%	4,67%
Desvio padrão anualizado	101,20%	70,98%	78,14%	75,94%
Variância	0,39%	0,19%	0,23%	0,22%
Assimetria	-0,24	-0,22	-0,17	0,10
Ex curtose	13,09	1,57	0,35	0,85
VaR99%	-17,64%	-12,92%	-14,23%	-15,28%
VaR95%	-8,37%	-7,60%	-8,14%	-7,60%

Na Tabela 4 vemos que as principais medidas estatísticas relacionadas com o risco, têm diminuído ao longo do tempo, sendo o mínimo ocorrido no horizonte a 5 anos. A exceção é no horizonte temporal a 3 anos que aumenta face aos 5 anos, voltando a diminuir no prazo mais curto, apesar dessa diminuição para a maioria das medidas os valores menores são encontrados no horizonte de 5 anos. Esse facto é devido a grande volatilidade do preço do *bitcoin* durante o ano de 2017 e 2018, que fez com que a tendência de diminuição do risco e volatilidade do ativo não fosse visível no horizonte temporal de 3 anos. Apesar dessa situação os valores a 3 anos são significativamente menores do que o do horizonte temporal mais longo.

Quando analisámos os máximos e mínimos dos retornos das amostras, verificamos que ambas as medidas têm diminuído ao longo do tempo. Tendo ambas o valor menor no horizonte temporal mais curto, o que mostra que os valores extremos das variações diárias do preço do *bitcoin* têm vindo a diminuir de amplitude.

Todos os períodos em estudo apresentam assimetria negativa menos no horizonte mais curto, em valor absoluto a assimetria tem sempre diminuindo, o que indica uma aproximação a distribuição normal dos retornos do *bitcoin*.

Em relação ao excesso de curtose, também, diminui-o ao longo dos horizontes mais curtos, tendo apenas aumentado no período de 1 ano fase ao de 3. Esta tendência de diminuição mostra que a distribuição dos retornos tem vindo a se aproximar da distribuição normal, não tendo as caudas tão pesadas como nos horizontes temporais mais longos.

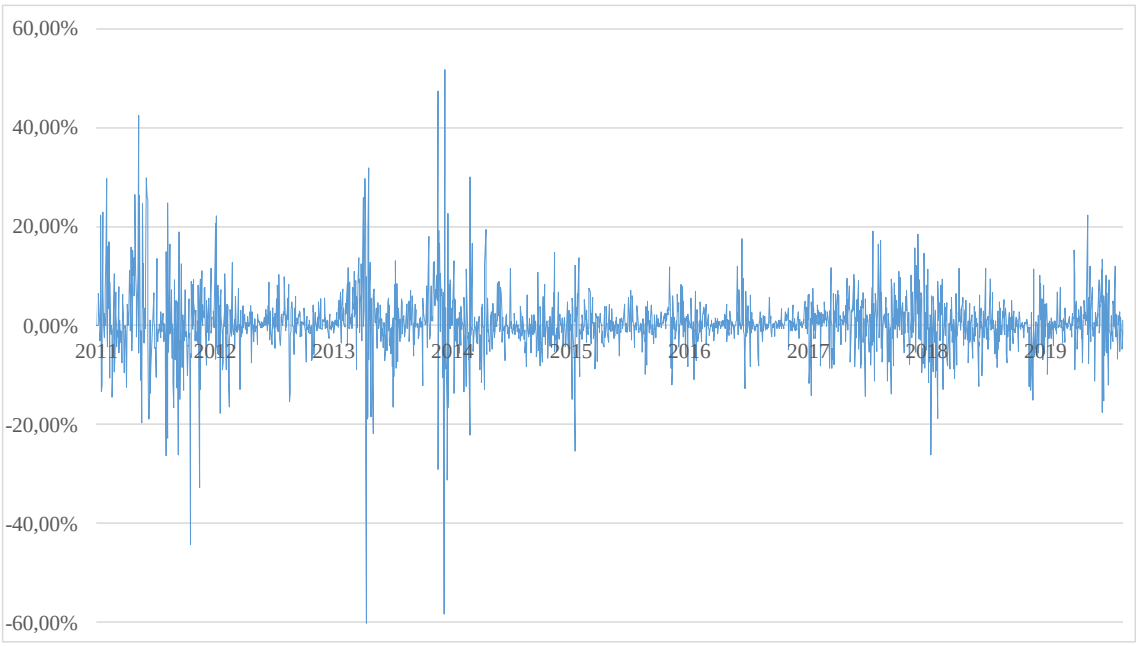
Quando se compara os valores do VaR este tem o menor valor para o período de 5 anos, sendo que no VaR a 95% o horizonte de 1 ano tem o mesmo valor do que o de 5 anos. O VaR para a mesma percentagem de perda espectável tende a ser menor nos horizontes mais longos, onde existem mais dados observáveis. Pelo que não se consegue retirar conclusões a partir deste dado.

Figura 13 - Evolução do preço do bitcoin em escala exponencial

Como as valorizações do preço do *bitcoin* são historicamente bastante elevadas, é difícil ver a diminuição do risco do ativo num gráfico com a evolução do preço na escala normal. É mais fácil de observar a diminuição das medidas de risco, através de um gráfico da evolução do preço do *bitcoin* em escala logarítmica, conforme mostrado na Figura 12.

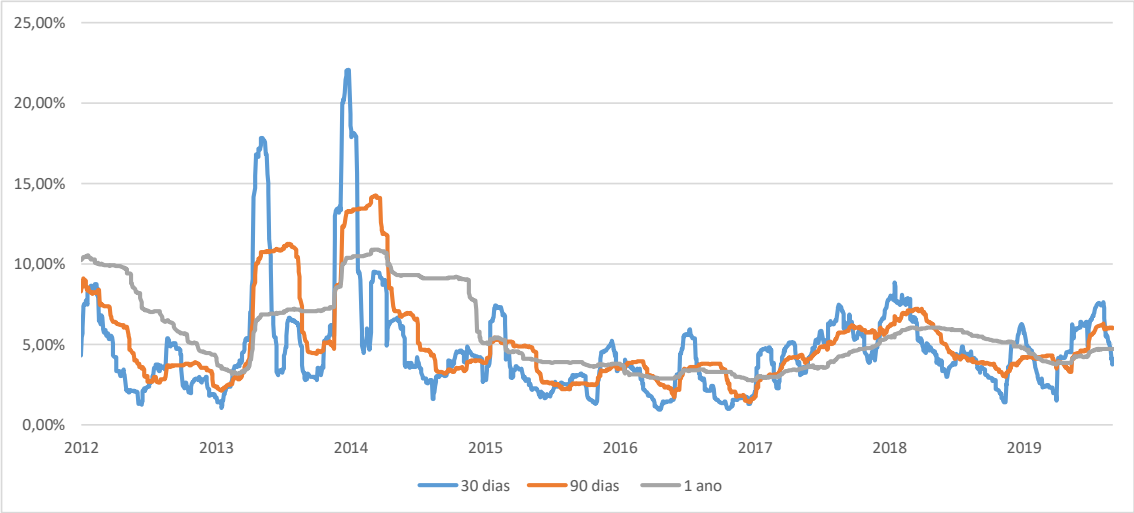
É visível que os movimentos extremos, quer de ganhos como de perdas, tem vindo a diminuir de magnitude e frequência. Com o ativo a ter um comportamento mais linear. O que é difícil de visível em escala normal, porque os valores absolutos de variação são tão elevados nos tempos recentes em relação aos tempos iniciais, que as variações no período inicial não são percetíveis.

Figura 14 - Logaritmo dos retornos diários do bitcoin



Quando analisamos apenas os retornos diários, figura 14 também é graficamente visível que as variações diárias têm diminuído de amplitude. Mesmo as grandes oscilações que resultaram do final da grande subida e posterior correção do final de 2017, em nada são comparáveis as oscilações iniciais do ativo e nos períodos de grandes subidas e quedas ocorridas durante os anos de 2013 e 2014.

Figura 15 - Evolução da volatilidade a 30, 90 dias e 1 ano do bitcoin



Comparado a evolução das volatilidades a 30 dias, 90 dias e 1 ano, figura 15, vemos que a volatilidade mostra uma tendência de redução a longo prazo, não existindo máximos de volatilidade tão elevados como no passado. Nos últimos períodos de subidas e correções, a volatilidade a 30 dias não ultrapassou os 10%, o que ocorreu nas duas grandes subidas de preço e posteriores correções de 2013 e 2014.

Na segunda parte do estudo é comparado os dados estatísticos e de VaR do *bitcoin* face aos restantes ativos analisados, bem como as correlações lineares entre os pares de ativos.

Tabela 5 - Analise estatística e VaR a 1 ano de diferentes ativos

	bitcoin	EUR	Ouro	MSCI World	EUR Bund 10Y	VIX
Média	0,13%	-0,02%	0,09%	-0,01%	0,01%	0,13%
Máximo	22,32%	0,90%	2,46%	3,04%	2,04%	36,43%
Mínimo	-17,53%	-1,06%	-1,82%	-2,48%	-2,21%	-19,81%
Desvio padrão diario	4,67%	0,36%	0,68%	0,80%	0,41%	8,17%
Desvio padrão anualizado	75,94%	5,78%	11,04%	12,90%	6,56%	132,02%
VaR99%	-15,28%	-1,05%	-1,53%	-2,44%	-0,99%	-19,64%
VaR95%	-7,60%	-0,64%	-1,02%	-1,59%	-0,57%	-11,34%

Em comparação com outras classes de ativos quando comparados os retornos no último ano, o *bitcoin* continua a ser o ativo mais arriscado. Apenas quando comparado com o VIX o risco é menor em todas as medidas. O VIX é uma medida especialmente volátil, construído e utilizado como *hedged* para os mercados financeiros, mais especificamente para o S&P 500. Excluindo o VIX o *bitcoin* apresenta quer maior desvio

padrão, quer maiores valores de VaR, do que todos os restantes ativos conforme é visível na Tabela 5.

O *bitcoin* apresenta um VaR a 99% mais de 15 vezes superior em relação ao EUR e ao EUR Bund 10Y, 11 vezes a do ouro e 6 vezes a do MSCI World. O que demonstra que apesar da redução da volatilidade e risco associado ao *bitcoin*, este continua a ser bastante mais arriscado que as classes de ativos tradicionais.

Tabela 6 - Correlação do bitcoin com outros ativos

Activo	*bitcoin*	EUR	Ouro	MSCI World	EUR Bund 10Y	VIX
bitcoin	1	0,1552**	0,1647***	-0,0525	0,1414**	0,1101*
EUR		1	0,5259***	0,0689	0,6433***	0,0342
Gold			1	-0,1888***	0,5057***	0,1955***
MSCI World				1	-0,0313	-0,7965***
EUR Bund 10Y					1	0,1202*
VIX						1

* indica significância ao nível de 10%
** indica significância ao nível de 5%
*** indica significância ao nível de 1%

Quando analisamos a correlação com outros ativos tabela 6, o *bitcoin* apresenta uma correlação linear baixa e em alguns casos negativa. A correlação é estatisticamente significativa ao nível de 1% em relação ao ouro, de 5% em relação ao EUR e EUR *Bund* 10Y e em 10% em relação ao VIX. Não foi encontrada evidencia estatística de correlação linear em relação ao MSCI *World*. Os valores apresentados estão de acordo com os resultados apresentados na literatura, em estudos para outros horizontes temporais e dados mais antigos. Com este nível de correlação linear quase nula e em alguns casos até negativa, faz com que o *bitcoin* possa ser utilizado como um ativo que aumenta a diversificação de uma carteira de investimentos devidamente diversificada.

7. Conclusões

Neste trabalho é apresentado a origem do dinheiro e do *Bitcoin*, bem como a interação entre tecnologia e economia que torna o *Bitcoin* uma das experiências mais inovadoras dos últimos anos. Apesar de ser uma tecnologia bastante recente, conseguiu vários avanços nestes 10 anos de existência, sendo talvez o mais impressionante de todos como uma tecnologia que é criada de forma espontânea e voluntária, consegue estar em funcionamento de forma contínua e interrupta durante os seus 10 anos de existência.

Desde a sua criação os indicadores do *Bitcoin* tiveram uma grande evolução, estando o poder de processamento, e consequentemente o nível de segurança do sistema, em máximos. O número de transferências e volume transferido em dólares também se encontra em valores elevados, bem como a sua capitalização bolsista. Este aumento da utilização tem levado a um aumento da liquidez e redução do risco financeiro associado à utilização do *bitcoin* como moeda e ativo financeiro.

Apesar de esta evolução, o *bitcoin* ainda se encontra longe de servir o propósito que o seu criado se propôs, de criar uma moeda e sistema de pagamento que viesse substituir o sistema monetário e financeiro atual. Para conseguir atingir esse objetivo a utilização do *bitcoin* terá que aumentar, aumentado a liquidez disponível e reduzindo a volatilidade para um nível em que o seu uso como moeda seja efetivo. Mesmo que esta experiência venha a acabar num futuro próximo, sem atingir os objetivos propostos, no mínimo consegui voltar a colocar em discussão o sistema monetário moderno, que dura desde a queda do padrão ouro.

Verificou-se que nos dados do ultimo ano, que o *bitcoin* continua a ter correlação baixa com diferentes ativos, o que está de acordo com estudos anteriores sobre o tema (Carrick, 2016) e (Guesmi et al., 2018), o que faz com que deva ser considerado pelos investidores como um ativo para adicionar à diversificação de uma carteira.

Em relação à utilização do *blockchain* ainda é cedo para se perceber quais as transformações que trará ao mundo. Os projetos que utilizam esta tecnologia ainda se encontram numa fase inicial, sendo difícil perceber se esta tecnologia poderá ser o início da nova revolução tecnológica.

Dada a grande volatilidade do *bitcoin*, sobretudo nos dados iniciais, é difícil tirar conclusões desse período. Devido também às grandes variações de preço, a construção de carteiras incluindo o *bitcoin* foram desconsideradas, pois, o peso do ativo na carteira iria ser apenas marginal.

Para trabalho futuro e dado a grande velocidade a que este mercado tem evoluído, deve ser estudado a relação do *bitcoin* com mais ativos financeiros e em diferentes condições de mercado. Devido à redução de risco que tem acontecido ao longo do tempo, deverá ser estudada a criação de portefólios diversificados que incluam *bitcoin* e outras moedas digitais, calculando a carteira de variância mínima, fronteira eficiente e a carteira de mercado, para vários horizontes temporais, de forma a medir qual o peso do *bitcoin* numa carteira diversificada, e como tem variado ao longo do tempo.

Será também interessante estudar como a introdução de novas tecnologias no protocolo do *Bitcoin*, nomeadamente a *lightning network*, influenciarão o crescimento e escalabilidade da utilização do *Bitcoin* e até que ponto influenciarão a sua utilização como moeda e ativo financeiro. Dado a grande quantidade de moedas virtuais existentes seria interessante fazer estudo idêntico ao realizado neste trabalho, em termos de risco e volatilidade para outras moedas virtuais, nomeadamente para o *ripple* e o *ethirion*, que são neste momento os principais concorrentes do *bitcoin*, em valor de mercado.

Referências bibliográficas

Ammous, S. (2018). ***The Bitcoin Standard - The Decentralized Alternative to Central Banking*.** JOHN WILEY & SONS INC.

Aristóteles. (1998). ***Política*.** Martin Claret.

Baur, D. G., & Dimpfl, T. (2017). **Realized Bitcoin Volatility.** ***SSRN Electronic Journal*.** https://doi.org/10.2139/ssrn.2949754

Baur, D. G., Hong, K., & Lee, A. D. (2018). **Bitcoin : Medium of exchange or speculative assets ?** *Journal of International Financial Markets, Institutions & Money*, *54*, 177–189. https://doi.org/10.1016/j.intfin.2017.12.004

Bitcoin Wiki. (2016). **Controlled supply - Bitcoin Wiki.** Retrieved May 20, 2019, from https://en.bitcoin.it/wiki/Controlled_supply

BitFury Group. (2015). **Proof of Stake versus Proof of Work**. Retrieved from http://bitfury.com/content/5-white-papers-research/pos-vs-pow-1.0.2.pdf

Bitstamp. (2019a). **Bitcoin Deposit.** Retrieved September 1, 2019, from https://www.bitstamp.net/account/deposit/bitcoin/

Bitstamp. (2019b). **Bitstamp tradeview.** Retrieved September 1, 2019, from https://www.bitstamp.net/market/tradeview/

blockchain. (2019a). **Confirmed Transactions Per Day.** Retrieved September 2, 2019, from https://www.blockchain.com/pt/charts/n-transactions?timespan=all

blockchain. (2019b). **Difficulty - Blockchain.** Retrieved September 1, 2019, from https://www.blockchain.com/pt/charts/difficulty?timespan=all

Blockchain. (2019a). **Blockchain Size.** Retrieved September 1, 2019, from https://www.blockchain.com/charts/blocks-size?

Blockchain. (2019b). **Distribuição da Taxa de Hash.** Retrieved September 6, 2019, from https://www.blockchain.com/pt/pools?timespan=4days

Blockchain. (2019c). **Estimated USD Transaction Value.** Retrieved September 5, 2019, from https://www.blockchain.com/pt/charts/estimated-transaction-volume-usd?timespan=all

Blockchain. (2019d). **Hash Rate.** Retrieved September 1, 2019, from https://www.blockchain.com/pt/charts/hash-rate?timespan=all

Blockchain. (2019e). **Median Confirmation Time.** Retrieved September 1, 2019, from https://www.blockchain.com/pt/charts/median-confirmation-time?timespan=all

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). **Bitcoin: Economics, Technology, and Governance.** *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brito, J., & Castillo, A. (2013). **Bitcoin: A Primer for Policymakers.** *Mercatus Center: Geroge Mason University.*, *29*(4), 3–12. https://doi.org/10.1017/CBO9781107415324.004

Carrick, J. (2016). **Bitcoin as a Complement to Emerging Market Currencies.** *Emerging Markets Finance and Trade*, *52*(10), 2321–2334. https://doi.org/10.1080/1540496X.2016.1193002

Catalini, C., & Gans, J. S. (2016). **Some Simple Economics of the Blockchain.** *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2874598

Coinmarketcap. (2019a). **Top 100 Cryptocurrencies by Market Capitalization.** Retrieved September 5, 2019, from https://coinmarketcap.com

Coinmarketcap. (2019b). **Total Market Capitalization.** Retrieved September 5, 2019, from https://coinmarketcap.com/charts/#dominance-percentage

Dai, W. (1998). ***b-money*.** https://nakamotoinstitute.org/literature/b-money/

data.bitcoinity.org. (2019). **Bitcoin exchanges.** Retrieved September 5, 2019, from http://data.bitcoinity.org/markets/exchanges/all/6m#volume_desc

ECB. (2012). ***Virtual Currency Schemes*.** https://doi.org/ISBN: 978-92-899-0862-7 (online)

FinCEN. (2013). **Application of FinCEN ' s Regulations to Persons Administering , Exchanging , or Using Virtual Currencies.** *Reports*, *100*(mm), 1–6. https://doi.org/March 18 2013

Fry, J. (2018). **Booms, busts and heavy-tails : The story of Bitcoin and cryptocurrency markets ?** *Economics Letters*, *171*, 225–229. https://doi.org/10.1016/j.econlet.2018.08.008

FSA.JP. (2017). **Decreto de revisão de uma parte da Ordem de Aplicação da Lei Bancária.** Retrieved February 24, 2017, from https://www.fsa.go.jp/news/28/ginkou/20170324-1.html

Fundchain. (2017). ***Distributed Ledger Technology: The genesis of a new business model for the asset management industry*.** Retrieved from https://theinvestmentinstitute.org/wp-content/uploads/2017/05/pwc-fintech-distributed-ledger-technology.pdf

Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). **Price manipulation in the Bitcoin ecosystem.** *Journal of Monetary Economics*, *95*, 86–96. https://doi.org/10.1016/j.jmoneco.2017.12.004

Gangwal, S. (2016). **Analyzing the Effects of Adding Bitcoin to Portfolio.** *World Academy of Science, Engineering and Technology, International Journal of Economics and Management Engineering*, *10*(10), 3519–3532.

Gangwal, S., & Longin, F. (2018). **Extreme movements in Bitcoin prices : A study based on extreme value theory.** *Working Paper Series*, 1–17. Retrieved from

https://www.longin.fr/Recherche_Publications/Resume_pdf/Gangwal_Longin_Extreme_movements_Bitcoin_prices.pdf

Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). **Is Bitcoin a Decentralized Currency?** *IEEE Security and Privacy*, *12*(3), 54–60. https://doi.org/10.1109/MSP.2014.49

Guesmi, K., Saadi, S., Abid, I., & Ftiti, Z. (2018). **Portfolio diversification with virtual currency: Evidence from bitcoin.** *International Review of Financial Analysis*, (September 2017), 1–7. https://doi.org/10.1016/j.irfa.2018.03.004

Hayek, F. A. (1976). ***Denationalisation of Money*.** Westminster: The Institute of Economic Affairs. Retrieved from www.bank-banque-canada.ca

Huang, S., & Carlsson, J. (2016). **Blockchain Technology in the Swedish Fund Market : A Study on the Trust Relationships Between Actors in a Blockchain-Based Fund Market.** Retrieved from http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1044630&dswid=-3933

Klein, T., Pham Thu, H., & Walther, T. (2018). **Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance.** *International Review of Financial Analysis*, *59*(May), 105–116. https://doi.org/10.1016/j.irfa.2018.07.010

Kristoufek, L. (2013). **BitCoin meets Google Trends and Wikipedia: Quantifying the relationship between phenomena of the Internet era.** *Scientific Reports*, *3*, 1–7. https://doi.org/10.1038/srep03415

May, T. C. (1988). **The Crypto Anarchist Manifesto.** ***Crypto Anarchy, Cyberstates, and Pirate Utopias.*** https://nakamotoinstitute.org/crypto-anarchist-manifesto/

Menger, C. (1892). **On the Origins of Money.** *Economic Journal*, *2*, 239–255.

Menger, C. (1976). ***Principles of Economics*.** Auburn: Ludwig von Mises Institute.

Mises, L. Von. (1953). **The Theory of Money and Credit.** *Library*.

Mishkin, F. (2010). **The Economics of Money and Banking.** Prentice Hall, 9 edition.

Nakamoto, S. (2008). **Bitcoin: A peer-to-peer electronic cash system.** Retrieved from www.bitcoin.org

Novais, C. (2018). ***Bitcoin e Blockchain - Introdução em 10 Passos*.** Chiado.

Platanakis, E., Sutcliffe, C., & Urquhart, A. (2018). **Optimal vs naïve diversification in cryptocurrencies.** *Economics Letters*, *171*, 93–96. https://doi.org/10.1016/j.econlet.2018.07.020

Ponsford, M. (2015). ***A Comparative Analysis of Bitcoin and other Decentralized Virtual Currencies : Legal Regulation in the People ' s Republic of China , Canada , and the United States*.** Retrieved from http://jolt.law.harvard.edu/digest/a-comparative-analysis-of-bitcoin-and-other-decentralized-virtual-currencies-legal-regulation-in-the-peoples-republic-of-china-canada-and-the-united-states

Portaldobitcoin. (2019). **Histórico das Principais Quedas do Bitcoin.** Retrieved September 1, 2019, from https://portaldobitcoin.com/historico-das-principais-quedas-do-bitcoin/

Prentis, M. (2015). **Digital Metal: Regulating Bitcoin As a Commodity.** *Case Western Reserve Law Review*, *66*(2), 609. https://doi.org/10.3868/s050-004-015-0003-8

Szabo, N. (2005a). **Bit gold.** *Unenumerated*, 2–3. Retrieved from http://unenumerated.blogspot.com/2005/12/bit-gold.html

Szabo, N. (2005b). **Shelling Out - The Origins of Money.** *Nick Szabo's Papers and Concise Tutorials*, 1–26. Retrieved from http://szabo.best.vwh.net/shell.html

Tasca, P. (2015). **Digital Currencies: Principles, Trends, Opportunities, and Risks.** *SSRN Electronic Journal*, 1–110. https://doi.org/10.2139/ssrn.2657598

Ulrich, F. (2014). ***BITCOIN - A moeda na era digital*.** Instituto Ludwig Von Mises Brasil. https://doi.org/10.1128/AAC.03728-14

Warwick, B. (2016). **Crypto as an asset class.** *Investment Advisor*, (October), 24–30.

Weber, W. E. (2016). **A Bitcoin Standard: Lessons from the Gold Standard.** *Bank of Canada Staff Working Paper*, *14*, 1–34. Retrieved from www.bank-banque-canada.ca

Wei, W. C. (2018). **Liquidity and market efficiency in cryptocurrencies.** *Economics Letters*, *168*, 21–24. https://doi.org/10.1016/j.econlet.2018.04.003

Wu, C. Y., & Pandey, V. K. (2014). **The Value of Bitcoin in Enhancing the Efficiency of an Investor's Portfolio.** *Journal of Financial Planning*, *27*(9), 44–52. Retrieved from http://eds.a.ebscohost.com.ezproxy.unal.edu.co/eds/pdfviewer/pdfviewer?sid=153c24ab-355a-4b53-bc87-d77a37864377@sessionmgr4002&vid=9&hid=4110

Yelowitz, A., & Wilson, M. (2015). **Characteristics of Bitcoin users: an analysis of Google search data.** *Applied Economics Letters*, *22*(13), 1030–1036. https://doi.org/10.1080/13504851.2014.995359

Yermack, D. (2013). ***IS BITCOIN A REAL CURRENCY? AN ECONOMIC APPRAISAL*.** Cambridge. Retrieved from http://www.nber.org/papers/w19747