



INSTITUTO SUPERIOR DE GESTÃO

**BITCOIN:
As inconsistências do modelo.**

GUILHERME CANEDO CORREIA

Dissertação a ser apresentada no Instituto Superior de Gestão, para o cumprimento dos requisitos necessários para obtenção do grau Mestre em Estratégias de Investimento e Internacionalização. .

Orientador: Professor Doutor Rui Moreira de Carvalho

Co-orientador: Mestre Joana Paulo Frazão

Lisboa

2017

RESUMO

A tecnologia Bitcoin, desenvolvida no final da década passada, em plena crise financeira, pretendeu ser, desde a origem, uma alternativa ao sistema financeiro vigente. Para Nakamoto, o criador do Bitcoin, o principal problema deste sistema reside no facto de ser necessária a presença de intermediários de confiança (v.g., instituições financeiras), para que as pessoas possam realizar transações financeiras. Esta configuração trilateral, paradigmática das transacções financeiras, leva a um aumento dos custos de transacção (desde logo, pela presença de uma terceira parte) mas também à necessidade de partilhar informação sobre as partes envolvidas (o que faz perigar a privacidade das pessoas).

Nakamoto apresenta, então, em 2008, um sistema de pagamentos *online* alternativo, baseado em código criptográfico e informático, mediante o qual seria possível (no seu entendimento) substituir os intermediários de confiança por uma confiança no código matemático. Por outro lado, e posto que as transações realizadas neste sistema alternativo são denominadas numa unidade própria, o Bitcoin, o sistema assume uma natureza dual: é simultaneamente um sistema de pagamentos, de troca, e uma moeda digital.

Com a presente dissertação pretendemos, por um lado, fazer uma revisão da literatura existente sobre o Bitcoin, e com isso perceber o estado da arte. Por outro lado, pretendemos também confrontar os objectivos que orientaram Nakamoto, no desenho do protocolo, com as evidências sobre o seu funcionamento.

Resumidamente, Nakamoto pretendeu desenvolver um sistema que fosse descentralizado, e acessível a qualquer pessoa: disso fez depender, inclusivamente, a segurança do próprio sistema. Não obstante, a arquitectura do sistema, a sua complexidade para o homem médio e as dinâmicas próprias do capitalismo parecem estimular a centralização. Com base na revisão de bibliografia realizada concluímos que existem vários níveis de centralização no sistema.

Ademais, ao escrever o protocolo do Bitcoin, Nakamoto introduziu um limite de emissão monetária, que será atingido em 2140, num total de 21 milhões de Bitcoins. Esta natureza deflacionária, da própria moeda, leva muitas pessoas a comprar Bitcoins como um investimento financeiro, aguardando a sua futura valorização. Ou seja, da já reduzida oferta monetária, uma grande parte não é utilizada para realizar transacções, resultando num mercado pouco líquido, e numa hipervalorização do Bitcoin (por confronto com outras moedas).

PALAVRAS-CHAVE:

BITCOIN, BLOCKCHAIN, MINERAÇÃO, DESCENTRALIZAÇÃO, MOEDA

ABSTRACT

Bitcoin technology, developed at the end of last decade, during the financial crisis, aimed to be an alternative to the current financial system. According to Nakamoto, the creator of Bitcoin, the main problem regarding this system resides in the fact that it requires the presence of trusted intermediaries (v.g., the financial institutions), so that a financial transaction can be made. This trilateral configuration of financial transactions, leads not only to the increase of transaction costs but also to the need of sharing information about the parties involved (which threatens people's privacy).

In 2008, Nakamoto presents an alternative online payment method, based on cryptography and informatics, through which it would be possible (in his knowledge) to replace the trusted intermediaries for the trust in the mathematic code. On the other hand, and since transactions made with this alternative system are denominated in a specific unit, the Bitcoin, the system assumes a dual nature: it is simultaneously a method of payment/exchange and a digital coin.

With the current dissertation we aim to make a literature review about Bitcoin and, in doing that, understand the state of the art. On the other hand, we want to confront the objectives that guided Nakamoto, in the protocol design, with the evidences of its functioning.

Briefly, Nakamoto aimed to develop a decentralized system fully accessible to anyone. This decentralization represents, on it's own, a security necessity, of the Bitcoin network.

Nonetheless, the system's architecture, its complexity to the average person and capitalism's own dynamics, seem to stimulate centralization. Based on the literature review, we can conclude that there are different levels of centralization in the system.

Furthermore, while writing the Bitcoin protocol, Nakamoto introduced a limit to the monetary supply, to be achieved by the year 2140, in a total of 21 million Bitcoins. This deflationary nature, leads numerous people into buying Bitcoins as a financial investment, hoarding them, for future profit. That is to say that, of the limited money supply, a substantial part isn't used to make transitions, resulting in a shortage of liquidity in the market, thus originating Bitcoin's hyper valorisation (when confronted with other currencies).

KEY WORDS:

BITCOIN, BLOCKCHAIN, MINING, DECENTRALIZATION, MONEY

AGRADECIMENTOS

É muito importante, para mim, começar esta Dissertação de Mestrado agradecendo a todos quantos, directa ou indirectamente, estiveram comigo ao longo deste processo, com os seus incentivos e incondicional apoio, sem os quais, este trabalho, jamais se tornaria uma realidade. Em primeiro lugar, uma palavra especial ao Professor Doutor Rui Moreira de Carvalho, meu professor e orientador, ao qual expresso o meu profundo agradecimento, pela sua amizade e orientação, que muito me ensinou e estimulou a querer saber mais; pelo seu profissionalismo, total apoio e doughtas opiniões e críticas, absolutamente determinantes à solução de todos os problemas que foram surgindo ao longo deste caminho. Pelo seu saber e incentivo permanente, foi um orgulho, uma honra tê-lo como orientador. Muito Obrigado!

Às Mestres, e amigas, Inês Frazão e Joana Frazão, que muito me ajudaram, com total disponibilidade e palavras positivas, nunca me deixando claudicar nos momentos mais difíceis. À minha mulher Joana, pelo seu carinho, força e apoio incondicional, uma luz na minha vida e em todos os momentos de maiores dúvidas e incertezas.

À minha Família, pelas oportunas manifestações de amor, companheirismo e encorajamento, mesmo tendo de abdicar da minha presença.

À minha querida irmã, Mané, em particular, que está sempre a torcer por mim!

Aos meus Amigos e a todos com quem fui trocando ideias... este trabalho é, em grande medida, devedor das vossas magníficas contribuições, da vossa curiosidade e, também, da paciência com que me ouviram... permitindo-me que fosse maturando perspectivas e conhecimentos.

E, por último, aos meus Colegas de Mestrado, meus amigos também, pelo entusiasmo partilhado.

A todos dedico este trabalho.

Muito Obrigado!

ÍNDICE

Resumo

Abstract

Agradecimentos

1. INTRODUÇÃO

1.1. Pergunta de partida e questões de investigação

1.2. Motivações

1.3. Metodologia

1.4. Estrutura

2. ENQUADRAMENTO DO TEMA

2.1. A economia digital

2.2. A moeda e o Estado

2.3. A crise financeira de 2008 e a regulação bancária

2.4. O fenómeno da confiança

3. BITCOIN

3.1. Antecedentes do Bitcoin

3.2. O sistema Bitcoin

3.3. Aspectos positivos, negativos, e desafios

3.3.1. Aspectos positivos

3.3.2. Aspectos negativos

3.3.3. Desafios

3.4. A regulação do sistema Bitcoin

4. INCONSISTÊNCIAS DO MODELO BITCOIN

4.1. A descentralização do sistema

4.1.1. A tendência de centralização

4.1.2. Impactos da centralização

4.2. A função de pagamentos e a unidade de conta

5. CONCLUSÕES

BIBLIOGRAFIA

WEBGRAFIA

Índice de Figuras

- Figura 1: aumento dos fluxos digitais.
- Figura 2: diagrama do sistema Bitcoin, com os vários tipos de nós

Índice de Quadros

- Quadro 1: crescimento empresas de base informacional
- Quadro 2: impacto da confiança na economia e nas transacções
- Quadro 3: confiança no sector financeiro
- Quadro 4: tipologia dos nós do sistema Bitcoin

Índice de Gráficos

- Gráfico 1: oferta monetária do sistema Bitcoin
- Gráfico 2: dimensão plataformas digitais
- Gráfico 3: evolução da confiança no Banco Central Europeu
- Gráfico 4: evolução da confiança na Comissão Europeia
- Gráfico 5: evolução da confiança no Parlamento Europeu
- Gráfico 6: evolução do poder de computação
- Gráfico 7: evolução da dificuldade do puzzle matemático
- Gráfico 8: valorização no período 2017-01-02 / 2017-06-26
- Gráfico 9: valorização no período 2017-01-02 / 2017-06-26
- Gráfico 10: Distribuição da taxa de hash (capacidade computacional), entre agrupamentos de mineiros (mining pools)
- Gráfico 11: crescimento das comissões de transacção.
- Gráfico 12: crescimento volume de transacções.

1. INTRODUÇÃO

O nosso objecto de estudo é o Bitcoin, em geral, e, em concreto, as dinâmicas específicas do seu sistema (o denominado Blockchain). Por conseguinte, diríamos que uma das nossas fontes primárias mais importantes, no sentido que lhes atribui Eco (1984, p. 65-66), é o documento em que tal sistema foi primeiramente apresentado. Falamos de *Bitcoin: A peer-to-peer electronic cash system*, publicado em 2008, assinado por Satoshi Nakamoto (entidade cuja verdadeira identidade ainda é actualmente desconhecida).

O entendimento do que seja o Bitcoin e a sua tecnologia é uma tarefa árdua, e pressupõe um conhecimento prévio de alguns conceitos informáticos, de engenharia de sistemas, matemáticos, entre outros. Citando Ulrich (2014, p. 15), “A tecnologia [Bitcoin] é tão inovadora, abarca tantos conceitos de distintos campos do conhecimento humano – e, além disso, rompe inúmeros paradigmas – que explicar o fenómeno pode ser uma missão ingrata.”

Não obstante, cabe aqui uma primeira indagação quanto à sua essência, o que fazemos com recurso às palavras do seu criador. No seu artigo fundacional, Nakamoto (2008, p. 1) começa por identificar os que considera serem os principais problemas do sistema de pagamentos vigente, que decorrem, em seu entendimento, das fraquezas inerentes ao modelo que se baseia na confiança (*inherent weaknesses of the trust based model*), isto, num contexto em que o comércio, em especial o comércio na Internet, depende de forma quase exclusiva das instituições bancárias para o processamento de transacções. Parafraseando, refere o Autor que o sistema actual não é compaginável com pagamentos irreversíveis, facto que promove um acentuar da função de mediação das instituições financeiras (Nakamoto, 2008, p. 1).

Ora, esta função mediadora implica um aumento dos custos de transacção, generaliza a necessidade de confiança, em especial a confiança nos intermediários, bem como, a necessidade de informação pessoal dos agentes económicos (que de outra forma não seria necessária) (Nakamoto, 2008, p. 1).

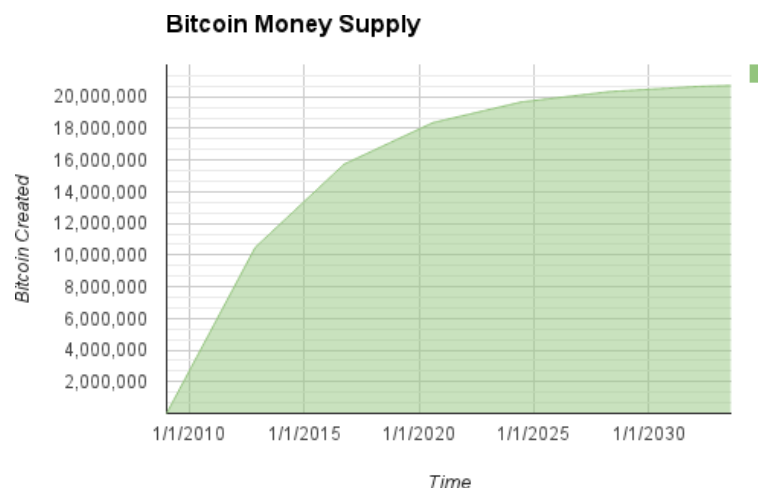
Este autor sugere, então, um sistema de pagamentos electrónico, baseado na criptografia (como suporte da confiança) e não na confiança em instituições, que permita aos utilizadores transacionar valor directamente entre si – sem a necessidade de um intermediário de confiança (Nakamoto, 2008, p. 1). Ou seja, trata-se de um sistema de pagamentos *online* entre pares (*peer-to-peer*) – sistema este que tem vindo a ser designado por Blockchain –, que utiliza uma unidade de conta própria (os bitcoins), e que torna redundante a intermediação de instituições financeiras.

Refere o mesmo autor, ainda, que o sistema apresentado é uma solução para o problema do gasto duplo (*double-spending*), mediante a implementação de um “peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.” (Nakamoto, 2008, p. 1). Simplificando esta ideia, e em tradução livre, podemos dizer que o autor se está a referir a uma forma de validação e certificação de transacções, com registo de data e hora, que funciona de forma distribuída/descentralizada entre os pares, sendo que tais transacções são registadas (em blocos sucessivos) mediante prova matemática criptográfica (computacional), desde a sua origem, ou seja, desde o bloco génese.

Além deste cariz descentralizado, e com relevância para o presente trabalho, importa referir, desde já, que o sistema Bitcoin foi concebido com um número predefinido de moedas (Nakamoto, 2008, p. 4), também designados bitcoins (grafado com minúscula) ou BTC. As moedas vão sendo geradas pelo sistema (a cada 10 minutos, aproximadamente), como prémio pela criação de blocos, até ao limite de 21 milhões de unidades (Tasca, 2016, p. 71) – no Gráfico 1, Antonopoulos (2014) apresenta o modelo de oferta monetária do sistema Bitcoin.

Gráfico 1: Oferta monetária do sistema Bitcoin

Fonte: Antonopoulos, 2014.



Acrescentamos, ainda, e seguindo Mougayar (2016, p. 1), que “em adição às suas potencialidades tecnológicas, os blockchains transportam consigo fundamentos filosóficos, culturais e ideológicos que também devem ser compreendidos”, razão pela qual, deve sublinhar-se que a compreensão do seu sistema reclama uma visão holística.

1.1. Pergunta de partida e questões de investigação

Para Quivy & Campenhoudt (2013, p. 44), “A melhor forma de começar um trabalho de investigação em ciências sociais consiste em esforçar-se por enunciar o projecto sob a forma de uma pergunta de partida. Com esta pergunta, o investigador tenta exprimir o mais exactamente possível aquilo que procura saber, elucidar, compreender melhor. A pergunta de partida servirá de primeiro fio condutor da investigação.”

Neste ensejo, podemos dizer que a nossa pergunta de partida nos remete para a tentativa de confrontar a ideia subjacente ao sistema Bitcoin com a prática que se tem verificado. Com efeito, em 2008, Nakamoto apresentou, fundamentalmente, um sistema de pagamentos *online* descentralizado, no qual circula uma unidade de conta própria¹.

No entanto, a arquitectura do sistema, quando combinada com as dinâmicas próprias do capitalismo, pode incentivar a ocorrência de um sistema não descentralizado (concentrado), como vários autores têm vindo a reconhecer, dos quais destacamos Beikverdi e Song (2015), Samtani e Baliga (2015), De Filippi e Loveluck (2016), Dodd (2017), Courtois e Bahack (2014), Shi (2016), Faggart (2015), Gervais, Karane, Capkun e Capkun (2014), Shin (2017), Cummings (2017), Buterin (2014), Kroll, Davey e Felten (2013).

Por outro lado, a mesma arquitectura pode incentivar, também, a utilização dos bitcoins como investimento financeiro, mais do que como instrumento de troca de um particular sistema de pagamentos, tal como tem sido sustentado, entre outros, por Guadamuz e Marsden (2014), Hanley (2015), Wu e Pandey (2014), Baek e Elbeck (2014).

Por conseguinte, cremos poder formular a nossa pergunta de partida da seguinte forma:

Q1: O modo de funcionamento (a prática) do sistema Bitcoin traduz o objectivo com que foi criado (a ideia)?

Considerando a natureza dual do Bitcoin, que desempenha uma função de sistema de pagamentos e outra enquanto moeda (Tasca, 2016), julgamos adequado e pertinente subdividir a pergunta de partida em duas questões de investigação. Estas questões traduzem a confrontação entre o modo de funcionamento do sistema Bitcoin e a ideia com que foi criado, sob dois prismas distintos (que correspondem à sua natureza dual): o primeiro, relativo à centralização/descentralização do sistema; o segundo, relativo à utilização das unidades de conta geradas pelo sistema.

Importa, acima de tudo, que estas questões de investigação sejam suficientemente claras, realistas e pertinentes (Quivy e Campenhoudt, 2013, p. 34-43), permitindo, assim, definir os

¹ Vide, Nakamoto (2008, p. 1).

instrumentos de análise (sejam qualitativos e/ou quantitativos) de forma adequada às respostas que se procuram.

Neste sentido, elencamos as duas questões de investigação que nos propomos investigar:

Q2: O sistema Bitcoin é descentralizado?

Q3: Os bitcoins são utilizados (maioritariamente) como meio de pagamento ou como investimento financeiro?

Assim, e no que respeita à segunda questão de investigação (Q2), propomo-nos indagar o funcionamento do sistema Bitcoin e do seu ecossistema, a forma de interacção entre os seus intervenientes, as regras de governação e decisão dentro do sistema, bem como, aferir a forma como o poder se encontra distribuído. Com este percurso, cremos ser possível ter uma ideia concreta do sistema, que nos permita saber se é centralizado ou descentralizado.

Relativamente à terceira questão de investigação (Q3), pretendemos perceber se as características desta moeda virtual incentivam maioritariamente a sua utilização como meio de pagamento, ou se incentivam um comportamento especulativo, na expectativa de ganhos futuros. Em concreto, importa perceber se o facto de se tratar de uma moeda com uma oferta limitada e pré-definida (21 milhões de unidades) tem impacto no comportamento dos utilizadores.

1.2 Motivações

A motivação principal que levou à escolha do presente tema encerra uma tentativa de compreensão da tecnologia Bitcoin, e dos seus impactos na sociedade, na esperança de conseguirmos, com isso, acrescentar conhecimento e divulgá-lo junto dos agentes económicos (e, esperamos nós, em seu benefício).

Com efeito, o potencial do Bitcoin enquanto instrumento de desintermediação na sociedade tem levado autores como Ross (2016, p. 89) a questionar se “existe um algoritmo para a confiança”², e a sustentar que “As novas formas de interacção estão a obrigar a uma reformulação do pacto estabelecido entre as corporações, os cidadãos e o Estado.” Para Ross (2016, p. 111), “A bitcoin (...) oferece um caso de estudo para o futuro da moeda, à medida que se intensifica a codificação do dinheiro.” No entanto, Ross (2016, p. 112), reconhece que “A bitcoin encapsula muitas das contradições e possibilidades das moedas digitais, num mundo que se define

² Neste sentido, Tapscott e Tapscott (2016, p. 5-6), referem mesmo que muitas pessoas estão, hoje em dia, a “tentar perceber as implicações de um protocolo que permite aos meros mortais produzir confiança através de um código inteligente.”, levando os mesmos autores a designar o protocolo do Bitcoin como o “Protocolo da Confiança”.

maioritariamente pelas economias e pelos governos nacionais.” Neste sentido, acreditamos que o estudo do sistema Bitcoin permitirá evidenciar quais sejam estas contradições, por um lado, e por outro, capacitar os agentes económicos com mais informação (que poderá ser útil nas respectivas tomadas de decisão).

Tapscott e Tapscott (2016, p. 6) focam-se na tecnologia que subjaz ao sistema Bitcoin (usualmente designada Blockchain), e defendem que essa tecnologia é o aspecto mais importante desta inovação, por permitir à internet da informação evoluir para a internet do valor e do dinheiro. Neste sentido, consideram os mesmos autores que o Bitcoin é a primeira expressão da Revolução Blockchain, uma vez que, o protocolo do Bitcoin é de fonte aberta (*open source*), permitindo a qualquer pessoa “fazer o [respectivo] download de forma livre e gratuita, executá-lo e usá-lo para o desenvolvimento de novas ferramentas para realizar transacções online. Enquanto tal, encerra o potencial de desencadear inúmeras novas aplicações e capacidades ainda não realizadas, com potencial de transformar muitas coisas.” Também focado na tecnologia subjacente ao Bitcoin, o Blockchain, Mougayar (2016, p. XXI) preconiza que “O blockchain não pode ser descrito unicamente como uma revolução. Ele é um fenómeno em curso, que avança lentamente como um *tsunami*, e que vai envolvendo tudo gradualmente ao longo do seu caminho por força do seu progresso.”

Estes possíveis enquadramentos, entre outros, e os impactos sociais que descrevem e anteveem, são, do nosso ponto de vista, motivação bastante para o estudo detalhado desta inovação.

Ademais, e considerando a juventude desta tecnologia, acreditamos também que a maioria dos agentes económicos ainda não está familiarizada com o tema (Vigna, Casey, 2016, p. 3-4).

Importa, portanto, desmistificar a tecnologia Bitcoin; criar conhecimento em nome do desenvolvimento. Seguindo Carvalho (2011, p. 180), “A noção de desenvolvimento está intimamente ligada ao processo de evolução e utilização da tecnologia. (...) A aplicação da ciência e da tecnologia (C&T), através do conhecimento, pode permitir mudanças estruturais com efeitos poderosos sobre o mercado e a distribuição dos recursos.”

Assim, se a primeira linha de força do presente trabalho passa pelo aprofundar do conhecimento da tecnologia Bitcoin, e do seu contexto social e económico, não podemos deixar de referir que se pretende, acima de tudo, construir uma narrativa crítica quanto à arquitectura do seu sistema (relativamente ao qual, julgamos existir uma inconsistência, relativa à descentralização do sistema), bem como, relativamente ao impacto das dinâmicas do próprio sistema capitalista no comportamento dos agentes económicos quanto à utilização dos bitcoins (relativamente ao qual julgamos existir outra inconsistência, em concreto, a preferência pela não utilização desta moeda, na expectativa de ganhos futuros).

Pelo exposto, e considerando os possíveis impactos do Bitcoin e da tecnologia Blockchain na sociedade, consideramos que o seu estudo é relevante no âmbito do Mestrado em Estratégia de Investimento e Internacionalização.

1.3. Metodologia

Aqui chegados, e para encontrarmos as respostas que o presente trabalho demanda, optámos por recorrer a uma metodologia de investigação qualitativa, que se traduz na adopção da revisão de literatura narrativa³ (Green, Johnson e Adams, 2006, p. 103; Ferrari, 2015, p. 230-231) como instrumento de investigação.

De forma sucinta, a revisão de literatura narrativa consiste numa análise crítica e objetiva da literatura existente sobre objecto de estudo. Conforme referem Green, Johnson e Adams (2006, p. 103), o tipo de revisão narrativa é útil para artigos científicos, uma vez que são conjugados vários aspectos relativamente ao objecto de estudo, de forma a conseguir-se uma visão de conjunto, abordando-se teoria e contexto, muitas vezes, de forma a provocar controvérsia.

Mediante a revisão da literatura narrativa pretendemos aprofundar o conhecimento sobre a tecnologia Bitcoin, destacar alguns dos estudos já realizados sobre o tema, tudo, com o objectivo de dar resposta às questões de investigação *supra*-referidas. Por outro lado, pretendemos, também, evidenciar as necessidades e os problemas já reconhecidos pelos diversos autores, relativamente ao tema que nos ocupa. Em suma, é nossa pretensão sintetizar, comparar e contrastar as várias perspectivas sobre o objecto de estudo, num todo coerente (Roberts, 2010, p. 100).

Esta dissertação resulta, em grande medida, da análise de diversos textos (trabalhos científicos, *papers* institucionais, dissertações de mestrado, teses de doutoramento, livros, *sites* da especialidade, revistas e jornais científicos e de renome, relatórios institucionais, entre outros), consultados em distintas plataformas e bases de dados, como sejam: ABI/INFORM, SSRN, Emerald, Springer, Elsevier, Google Scholar, e ProQuest.

Utilizámos como palavras-chave da pesquisa, na primeira fase, apenas a palavra Bitcoin, para que pudéssemos ter uma visão ampla do estado da arte. Na segunda fase, e com o objectivo de focarmos a pesquisa, utilizámos como palavras-chave as seguintes combinações: Bitcoin + *network*, Bitcoin + *decentralization*, Bitcoin + *mining*, Bitcoin + *price volatility*, Bitcoin + *deflation*, e Bitcoin + *hoarding*.

1.4. Estrutura

A presente dissertação seguirá a seguinte estrutura. No segundo capítulo, faremos um enquadramento do tema, com especial enfoque em conceitos como a economia digital (uma vez que o Bitcoin é, para todos os efeitos, uma tecnologia digital, recorre a ferramentas digitais, e consiste num instrumento de comércio e de transacções), a moeda e a sua relação com o Estado (em virtude de o Bitcoin ser, também, uma moeda digital), a crise financeira de 2008 e a regulação bancária (tanto pelo facto de o Bitcoin ter surgido em 2008, no seio da crise financeira, como uma alternativa ao sistema vigente, mas também pelo facto de as soluções regulatórias serem enunciativas relativamente aos problemas existentes no sistema financeiro), e, por fim, a confiança (por se tratar de um conceito constitutivo da crítica de Nakamoto ao sistema vigente, e por se considerar que o protocolo do Bitcoin codifica a confiança).

Depois, no terceiro capítulo, versaremos o Bitcoin e o seu ecossistema. Tentaremos apresentar, de forma cabal, as características do sistema e da moeda digital, e apresentaremos os estudos feitos sobre o tema, por vários autores. Começaremos pelos antecedentes do Bitcoin (onde procuraremos evidenciar as tentativas prévias de criação de dinheiro virtual, bem como, os seus contributos para o sucesso do Bitcoin). De seguida, mergulharemos no sistema Bitcoin, onde tentaremos evidenciar as suas características. Posteriormente, caberá uma exposição relativa aos aspectos positivos e negativos do Bitcoin (sobre vários pontos de vista e considerando a sua natureza dual). Por fim, importará também detalhar a forma como as instituições governamentais veem o sistema Bitcoin, como pretendem regular esta tecnologia, e qual o estatuto jurídico que lhe atribuem.

No quarto capítulo, faremos a confrontação entre os objectivos da criação do Bitcoin (sistema de pagamentos e moeda digital) e a realidade do seu funcionamento. Pretendemos aqui apresentar os autores que também seguiram este caminho, e que procuraram a realidade dos factos, mais do que a reprodução gratuita de ideias preconcebidas. Seguiremos aqui, como se referiu *supra*, a natureza dual do Bitcoin: num primeiro momento, quanto ao sistema de pagamentos, indagaremos se é verdadeiramente descentralizado (uma das condições de segurança do sistema, segundo Nakamoto (2008, p. 1)); depois, num segundo momento, relativamente ao Bitcoin enquanto moeda digital, tentaremos discernir se cumpre a função de moeda e se a arquitectura do sistema induz uma utilização como investimento financeiro (mais do que como unidade de troca no âmbito de um sistema de pagamentos específico).

Por fim, no quinto capítulo, apresentaremos as nossas conclusões, e enunciaremos as avenidas de investigação futura.

2. ENQUADRAMENTO DO TEMA

Com o presente capítulo, é nosso objectivo conferir ao presente estudo um enquadramento histórico e conceptual, que permita compreender o Bitcoin e o seu aparecimento. No fundo, pretendemos inserir o tema no seu contexto histórico, social e tecnológico, na esperança de conseguirmos uma visão holística e compreensiva do fenómeno.

2.1. A economia digital

A história da humanidade tem sido marcada pelas necessidades vividas pelo ser humano e pela aplicação do seu engenho e conhecimento na respectiva satisfação. Maslow (1954, p. 35-58) identifica as necessidades humanas como as principais causas da acção humana, distinguindo entre necessidades fisiológicas, de segurança, de amor e relacionamento, de estima, e, por fim, de realização pessoal, organizadas numa estrutura piramidal – na base da pirâmide, as fisiológicas, necessidades cuja não satisfação impossibilita a vida, até ao topo da pirâmide, onde encontramos as necessidades de realização pessoal (cuja satisfação não é tão premente como todas as anteriores). Assim, podemos sustentar que o ser humano procurou, sempre, prover às suas necessidades e aumentar o seu bem-estar, a sua qualidade de vida, recorrendo, para o efeito, ao aproveitamento de recursos naturais e humanos, ao desenvolvimento de ferramentas, à organização em comunidades, à partilha de conhecimento (num grau crescente de complexificação).

A evolução da humanidade pode ser dividida em períodos históricos, marcados por diferentes características e culturas. Toffler (1980, p. xxii) identifica três vagas da evolução da humanidade, divisão que permite, segundo o mesmo autor, ter uma melhor visão de conjunto⁴: a primeira vaga corresponde à fase de predomínio da agricultura; a segunda vaga corresponde à fase industrial, resultado da revolução industrial (século XVIII); a terceira vaga, materializa-se numa fase pós-industrial, e identifica-se com a sociedade da informação (com início por volta da década de 50, do século XX). Para Toffler (1980, p. 19-28), a sucessão de vagas deve-se, essencialmente, ao tipo de energia utilizada, às inovações (científicas e tecnológicas), e ao sistema de comunicações (da informação e de pessoas e bens), com todas as consequências sociais, institucionais, políticas e económicas daí resultantes.

⁴ Toffler (1980, xx e xxii) refere-se a “sínteses de larga escala”.

Toffler (1980, p. 128-130) distingue as indústrias da segunda vaga (carvão, caminhos-de-ferro, aço, entre outras) – baseadas em princípios electromecânicos simples, elevados gastos energéticos, desperdício e poluição, trabalho pouco qualificado e repetitivo, bens standardizados e controlos centralizados – das indústrias da terceira vaga (computação e processamento, aeroespço, petroquímica, semicondutores, comunicações avançadas, entre outras) – muito mais eficientes de um ponto de vista energético e mais complexas a nível de conhecimento (entre outras características).

Por outro lado, a evolução da sociedade industrializada costuma ser dividida em períodos históricos, de acordo com as revoluções industriais que se sucederam, desde meados do século XVIII. Seguindo Schwab (2017, p. 6-7), a primeira revolução industrial situa-se entre 1760 e 1840, e foi provocada pelo desenvolvimento dos caminhos-de-ferro, pela invenção do motor a vapor, e pela produção mecânica que o motor a vapor permitiu. A segunda revolução industrial começou no fim do século XIX, terminando por volta dos anos 60, do século XX. Aqui, o advento da electricidade e das linhas de montagem permitiu a produção em massa. A terceira revolução industrial, iniciada a partir dos anos 60, foi fruto do desenvolvimento dos semicondutores, computadores (nomeadamente, os computadores pessoais), e da internet.

O papel da informação e do acesso ao conhecimento foi determinante em todos estes momentos históricos, ou, se se preferir, em todas as referidas transições⁵. Neste sentido, Drucker (2007, p. 41-42) destaca a transformação do conhecimento (e do seu acesso e divulgação) registada na sociedade inglesa, durante o período da primeira revolução industrial, e a forma como essa transformação mudou a economia:

“entre 1750 e 1800, o Reino Unido deixa de considerar as patentes como monopólios para enriquecer os favoritos do rei a registá-las, como forma de encorajar a aplicação do conhecimento às ferramentas, aos produtos, e aos processos, tendo em vista compensar os inventores, desde que publicassem as suas invenções. Isto não se limitou a desencadear um século de criação mecânica febril no país: acabou com os mistérios e com o secretismo dos ofícios. (...) Foi esta mudança no significado do conhecimento que tornou o capitalismo moderno inevitável e dominante. Acima de tudo, a rapidez da mudança da técnica

⁵ Considerando a importância que a informação e a transmissão de conhecimentos desempenharam na evolução da humanidade (ou das sucessivas civilizações), não podemos deixar de referir a invenção da escrita como uma das mais importantes tecnologias inventadas pelo ser humano. Para Harari (2017, p. 182-187), a invenção da escrita e do dinheiro, pelos sumérios, há cerca de 5000 anos, permitiu ultrapassar as limitações de processamento de informação do cérebro humano. A informação tornou-se mais complexa, uma vez que podia ser registada. Por outro lado, isso permitiu criar estruturas sociais maiores, mais complexas e burocráticas, assentes em regulamentos e protocolos. Floridi (2016, p. 1), que divide a evolução do desenvolvimento humano em três idades (pré-história, história e híper-história) refere mesmo que a criação da escrita marca a mudança da pré-história para a história, considerando que só a partir dessa invenção foi possível registar eventos e acumular e transmitir informação para consumo futuro.

criou uma procura de capital muito superior à que os artífices conseguiam oferecer. A nova tecnologia também exigia concentração da produção, o que significava uma mudança para a fábrica.”

Por outro lado, Drucker (2007, p. 46-53) enquadra ainda o conhecimento no âmbito da revolução da produtividade. Num primeiro momento, o conhecimento “começou por ser aplicado às ferramentas, aos processos e aos produtos.” Depois, numa segunda fase, o conhecimento começou a ser aplicado ao trabalho, o que permitiu criar “economias desenvolvidas, dando assim início à explosão de produtividade”. Por fim, num terceiro momento, o conhecimento começa a ser aplicado ao conhecimento:

“a Revolução da Produtividade já terminou. Há quarenta anos, por volta de 1950, as pessoas que se ocupavam em fazer movimentar coisas ainda eram a maioria em todos os países desenvolvidos. Em 1990, já haviam diminuído para um quinto da força de trabalho. (...) Aumentar a produtividade dos trabalhadores manuais na indústria, na agricultura e nos transportes deixou de ser um factor de criação de riqueza só por si. (...) A partir de agora, o que interessa é a produtividade dos trabalhadores não manuais. E para isso é preciso aplicar conhecimento ao conhecimento.”

Em sentido concordante, Castells (2002, p. 30-31) refere que a informação e o conhecimento foram centrais nas primeira e segunda revoluções industriais. No entanto, “o que caracteriza a actual revolução tecnológica não é a centralidade do conhecimento e da informação, mas a aplicação desses conhecimento e informação à criação de aparelhos geradores de conhecimento e de processamento/comunicação de informação, num círculo de feedback cumulativo entre a inovação e as utilizações da inovação.”

Acrescenta Drucker (2007, p. 55-59) que “o conhecimento é hoje o único recurso com significado. Os tradicionais «factores de produção» (...) não desapareceram, mas tornaram-se secundários”. Esta transformação do conhecimento e do objecto em que é aplicado (o próprio conhecimento) permite a inovação sistemática e intensifica a especialização (pressupondo esta última a sua organização em disciplinas)⁶.

A transformação do conhecimento (e da sua aplicação), aliada ao desenvolvimento das novas tecnologias de informação e comunicação, tem vindo a provocar profundas mudanças na sociedade e na economia, levando Schwab (2017, p. 1-7) a acreditar que estamos a assistir, hoje em dia, ao início de uma quarta revolução industrial, marcada pelo advento das tecnologias digitais, a qual implica, em seu entendimento, uma mudança de paradigma social,

⁶ “Uma disciplina converte um “ofício” em metodologia (...). Cada uma destas metodologias transforma a experiência *ad hoc* em sistema. Cada uma converte o episódio em informação. Cada uma converte a técnica em algo que pode ser ensinado e compreendido.” (Drucker, 2007, p. 59).

nomeadamente, quanto à forma como comunicamos, como nos expressamos, como nos informamos e entretemos, e que as alterações em curso são inéditas em termos de dimensão, de velocidade e de âmbito⁷. Castells (2002, p. 28-29 e 70-72) também considera, na linha das investigações de Carlota Perez, Christopher Freeman e Giovanni Dosi (que adaptaram ao campo económico, a análise das revoluções científicas, de Thomas Kuhn⁸) que as novas tecnologias⁹, especialmente as desenvolvidas a partir da década de 60, do século XX, encerram um novo paradigma¹⁰ tecnológico, com as seguintes características: a informação é um bem e as tecnologias actuam sobre informação; os efeitos das novas tecnologias são onnipresentes, afectando todos os aspectos da vida social; a lógica de rede pode ser aplicada a todos os processos e organizações, permitindo crescimentos exponenciais¹¹; assenta na flexibilidade, uma vez que os processos digitais são facilmente alterados (são facilmente adaptáveis); por fim, as várias tecnologias convergem num sistema altamente integrado.

A sociedade resultante desta confluência, de conhecimento aplicado a conhecimento e de tecnologias de informação e comunicação, tem sido descrita de várias formas: a sociedade super-industrial, de Toffler; a sociedade pós-capitalista, de Drucker; a sociedade da informação

⁷ Também neste sentido, Innerarity (2011, p. 35) defende que “Estamos a viver uma época especialmente acelerada”, provocada pelas “novas tecnologias da instantaneidade” que deram origem a “uma cultura do presente absoluto sem profundidade temporal. A origem desta relação com o tempo encontra-se na aliança estabelecida entre a lógica do lucro imediato, própria dos mercados financeiros, e a instantaneidade dos meios de comunicação.” A aceleração social descrita por Innerarity é causa da incapacidade política actual, porquanto impede a sociedade de “levar o futuro a sério” (ibidem, p. 30), já que, não existindo, no horizonte temporal, o longo prazo, se perde o espaço da estratégia (“transformam a acção pública em reacção pública”).

⁸ Para Kuhn (2009, p. 13), os paradigmas são “realizações científicas universalmente reconhecidas que durante um certo período fornecem problemas e soluções-modelo para uma comunidade de especialistas.” No posfácio da edição de 2009, Kuhn (2009, p. 244-256) densificou o conceito de paradigma, em resposta a alguns críticos, sustentando que os paradigmas são uma constelação dos comprometimentos de grupo, e também exemplos e valores partilhados por um grupo. Nas palavras de Rifkin (2016, p. 25), “Kuhn descreveu um paradigma como sendo um sistema de crenças e pressupostos que funcionam em conjunto para estabelecer uma visão do mundo integrada e singular de forma tão convincente e entusiasmante que é entendida como equivalente à própria realidade.”

⁹ A respeito da origem etimológica da palavra tecnologia, ver Cunha (1986, p. 759 e 480): do grego “*technê*” (arte, habilidade) e “*lógos*” (palavra, estudo, tratado).

¹⁰ Han (2016, p. 1-17) defende, num tom pessimista (“uma nova crise”), que estamos a viver uma “radical mudança de paradigma”, consequência das inovações digitais. Com efeito, refere este autor que “O meio digital, enquanto tal, *privatiza* a comunicação, na medida em que desloca a produção de informação do público para o privado.” Por outro lado, “A interconexão digital favorece a comunicação simétrica”, prejudicando a eficácia do poder, porquanto o poder encerra uma relação assimétrica, baseada na hierarquia. Por outro lado, Han (2016, p. 27) sustenta que “O meio digital é um meio de presença. A sua temporalidade é o presente imediato.” Este facto leva à limitação de intermediários: “Qualquer instância de mediação é cada vez mais firmemente excluída. A mediação e a representação são percebidas como opacidade e ineficácia, como factor de congestionamento dos fluxos temporal e da informação.” Por fim, põe em evidência a dupla qualidade do cidadão digital, enquanto consumidor e produtor – transparece aqui uma clara evocação ao conceito de Toffler de prosumidor (1980, p. 251).

¹¹ O efeito de rede (*network effects*), apresentado por Robert Metcalfe, sustenta que uma rede é exponencialmente mais valiosa quantos mais participantes tiver (Castells, 2002, p. 71). Trata-se, portanto, de uma externalidade positiva.

ou sociedade em rede, de Castells; a híper-história, de Floridi; a idade da inteligência em rede, de Tapscott¹²; entre muitas outras descrições ou qualificações. Para Dias (2014, p. 23), “Comum a todos estes conceitos é o reconhecimento da importância das tecnologias da informação e da comunicação (TIC) como um dos elementos mais importantes, quando não mesmo o principal, na descrição da sociedade em que vivemos.”

Assim, podemos dizer que as inovações tecnológicas têm vindo a transformar a sociedade, fruto da sua capacidade para satisfazer as necessidades dos seres humanos¹³, criando novos produtos e serviços, novas formas de organização, novas formas de produção de energia, de comunicação, de forma mais barata, mais eficiente, mais rápida. Importa recordarmos, aqui, que os recursos são escassos, por natureza, razão pela qual, as pessoas procuram fazer o melhor aproveitamento possível dos recursos ao seu dispor (Bento, 2004, p. 78-79).

Por outro lado, a capacidade de as sociedades dominarem as inovações tecnológicas tem forte impacto no seu sucesso, e na capacidade de se transformarem, e de serem competitivas num mundo caracterizado pela escassez de recursos (Castells, 2002, p. 7-13). Esta observação é tanto mais evidente, quando consideramos que o progresso tecnológico tem intensificado os processos de globalização das economias (ou seja, tem potenciado a “integração e a interdependência das diversas economias nacionais, através da eliminação de barreiras ao comércio e aos movimentos de capitais”¹⁴, de pessoas e bens). Para Bento (2004, p. 94), “é natural que como principal facilitador, senão mesmo estimulante, do processo de globalização tenha funcionado sobretudo o progresso tecnológico, nomeadamente na área dos transportes, das comunicações e do tratamento da informação, acompanhado por políticas públicas mais disponíveis à abertura das respectivas economias.” Bento (2004, p. 96) sustenta, inclusivamente, e de forma expressiva, que “a acelerada evolução verificada nas tecnologias dos transportes, das comunicações e da informação, desvalorizou a importância da localização das actividades produtivas.”, razão pela qual, numa economia globalizada, aberta e interdependente, como a actual, o domínio das inovações tecnológicas é condição de sucesso e da capacidade de competir.

Esta evolução social e económica não é regular, antes assume uma natureza cíclica. A teoria económica tem estudado e demonstrado que estes ciclos são provocados (maioritariamente) por inovações tecnológicas. Com a análise destes ciclos pretende a teoria económica justificar o desenvolvimento e o crescimento económicos. Como referem Samuelson e Nordhaus (2005, p.

¹² Vide, Tapscott (2015, p. 11-17).

¹³ Como afirma McQuivey (2013, p. 7), as inovações, isoladas, não criam grande valor, até ao momento em que conseguem ser disruptivas.

¹⁴ Vide, Bento (2004, p. 93).

466), “A compreensão dos ciclos económicos tem sido um dos problemas mais persistentes da macroeconomia”, sendo definidos, usualmente, como “flutuações do produto, do rendimento e do emprego nacionais, com uma duração habitual de 2 a 10 anos, caracterizada pela expansão ou contracção generalizadas na maioria dos sectores da economia.” (Samuelson e Nordhaus, 2005, p. 468). Apesar de não caber no âmbito do presente trabalho uma investigação exaustiva sobre os ciclos económicos, destacamos, as ideias de Schumpeter, uma vez que este autor tentou explicar o crescimento económico como resultado da inovação (do progresso técnico), a qual seria empreendida pelo empresário¹⁵, ou seja, “pela pessoa que inova” (Diniz, 2010, p. 104). Segundo Diniz (2010, p. 104), o que subjaz à inovação, na lógica schumpeteriana, “é a introdução de uma nova maneira de utilizar os recursos produtivos da economia”, a qual levará ao crescimento económico depois de introduzida na sociedade pelo empresário, fase que Schumpeter designa como “destruição criadora”¹⁶.

O trabalho de Schumpeter beneficiou dos estudos prévios de Kondratieff, que apresentava “o capitalismo como sendo caracterizado a longo prazo por um encadeamento de períodos de cerca de 50 anos, decompondo-se em duas fases quase iguais, uma de forte crescimento, pleno emprego e ligeira inflação, outra de estagnação, desemprego e deflação.” (Daniel, 2013, p. 110). Kondratieff (1982, p. 107-111) fundamentou a sua análise, essencialmente, em dados estatísticos relativos ao nível de preços, à taxa de juro, ao salário médio, entre outros indicadores, e considerava que os ciclos longos eram causados pelas características intrínsecas do sistema económico, e não por factores externos (como sejam, as inovações científicas, as guerras, descobertas de novos mercados ou de jazidas de ouro) (Kondratieff, 1982, p. 151-154). Schumpeter “Substitui a abordagem financeira [de Kondratieff], centrada nos preços, que reserva para o ciclo de média duração, por uma abordagem ligada à evolução do progresso técnico. O ciclo de Kondratieff revisto e corrigido por Schumpeter é um ciclo de produtividade. Na origem do crescimento está aquilo a que Schumpeter chama uma «nova combinação».” (Daniel, 2013, p. 110). Na verdade, Schumpeter desenvolve a sua teoria do crescimento económico conciliando os ciclos longos, de Kondratieff, com os ciclos de curto e médio prazo (Daniel, 2013, p. 110), pois entendia que os vários ciclos são importantes para se compreender a evolução da economia.

Vemos, assim, que para Schumpeter o progresso tecnológico é um factor decisivo da produtividade e, conseqüentemente, do sucesso das sociedades e da melhoria do nível de vida

¹⁵ Segundo Daniel (2013, p. 107), a palavra *empresário* terá sido introduzida por Richard Cantillon, caracterizando-se a sua actividade “pelo facto de os seus custos serem certos, ao passo que os benefícios são incertos. O que faz o seu mérito é passar o tempo a gerir a incerteza.”

¹⁶ Vide, também, Brynjolfsson e Saunders (2010, p. x).

das populações. Também Brynjofsson e Saunders (2010, p. xi) destacam que a tecnologia (especialmente, a tecnologia de informação e comunicação) foi a causa principal do ressurgimento da produtividade, desde 1995, nos Estados Unidos da América – estes autores sublinham, porém, que o grande impacto da tecnologia beneficiou da implementação de práticas de negócio orientadas para a produtividade.

A combinação das novas tecnologias de informação e comunicação, digitais, e a sua propagação na sociedade, de forma globalizada, levaram Don Tapscott, em 1995, na sua obra *The digital economy* (Tapscott, 2015, xiii), a cunhar e a desenvolver o conceito de economia digital. O advento da internet e a difusão dos computadores pessoais (entre outros avanços tecnológicos) marcam o início de uma nova era, que permitiu a criação de uma rede global (conectividade), e possibilitou a realização de transacções comerciais mais baratas, rápidas e mais eficientes, feitas em plataformas digitais, o que revolucionou a forma de fazer comércio (*e-commerce*) (entre outros, Castells, 2002, p. 38-51; Tapscott, 2015, p. 2-4; Harari, 2017, p. 436-437; Plassaras 2013, p. 379; Ayres e Williams, 2003, 317-329)¹⁷. Para Bheemaiah (2017, p. 158-159), os profundos impactos da tecnologia na sociedade e no progresso estão a acelerar, inclusivamente, o ritmo dos já referidos ciclos económicos, em grande medida provocados pela diminuição dos custos de produção (lei de Wright)¹⁸. Invoca, para justificar esta observação, a diminuição do custo dos transístores (lei de Moore)¹⁹, que permitiu um grande desenvolvimento da capacidade dos computadores, levando à ubiquidade da sua presença, a nível global. A ubiquidade dos computadores, e a socialização que permitiu, levou, por sua vez, à complexificação das redes (Castells, 2002, p. 70-71; Bheemaiah 2017, p. 158-159; Langley e Leyshon, 2016, p. 2).

Não obstante, como reconhecem Tsyganov e Apalkova (2016, p. 296), o conceito de economia digital é ambíguo, existindo diversas definições e entendimentos. Por exemplo, no relatório relativo à economia digital, do *Business, Innovation and Skills Committee*, da *House of Commons* (2016, p. 4), sustenta-se que, o conceito de economia digital abrange, não apenas o acesso digital a mercadorias e serviços, mas também, a utilização da tecnologia digital. Já a OCDE (2012, p. 5) concebe a economia digital como mercados assentes em tecnologias digitais, que facilitam o comércio de bens e serviços através do comércio eletrónico.

¹⁷ Segundo a OCDE (2012, p. 5) “A expansão do sector digital tem sido um dos principais impulsionadores do crescimento económico nos últimos anos, e a mudança para um mundo digital teve efeitos sobre a sociedade que se estende muito além do contexto da tecnologia digital sozinho.”

¹⁸ A lei de Wright, apresentada em 1936, prevê a diminuição dos custos de produção, à medida que o progresso tecnológico aumenta de forma exponencial (Bheemaiah, 2017, p. 159).

¹⁹ A lei de Moore (revista), apresentada em 1965 por Gordon Moore, sustenta que o número de transístores inseridos num *microship* duplicam a cada dois anos (Brynjofsson e Saunders, 2010, p. ix).

Assim, a economia digital tem por base a utilização das tecnologias da informação e da comunicação, onde se podem incluir, nomeadamente, a internet, a micro-eletrónica, a computação (*hardware* e *software*), as telecomunicações, fibra óptica, comunicação electrónica, comunicação *wireless*, a nanotecnologia, a *Internet of Things* (IoT), a *web* e *web 2.0*, as plataformas digitais, o *cloud computing*, os telemóveis, os *smartphones*, os *tablets*, os ecrans tácteis, a tecnologia *wearable*, o GPS, a realidade virtual, a realidade aumentada, os *drones*, as impressoras 3D, a automação, a robotização, o *Big Data*, as redes sociais, a Inteligência Artificial, a biotecnologia, a computação quântica (*vide*, entre outros, Castells, 2002, p. 29; Schwab, 2017, p. 1; Floridi, 2016, p. vi; Dias, 2014, p. 24). É a combinação destas tecnologias que leva Schwab (2017, p. 13-25), como se referiu *supra*, a defender a existência de uma quarta revolução industrial.

Podemos incluir aqui, enquanto tecnologias da comunicação e da informação, e, acima de tudo, enquanto tecnologias digitais, as moedas digitais e o Blockchain (neste sentido, McMillan, 2014, p. 125; Tapscott e Tapscott, 2016; Skinner, 2016, p. 1; Bheemaiah, 2017, p. 92 e 160).

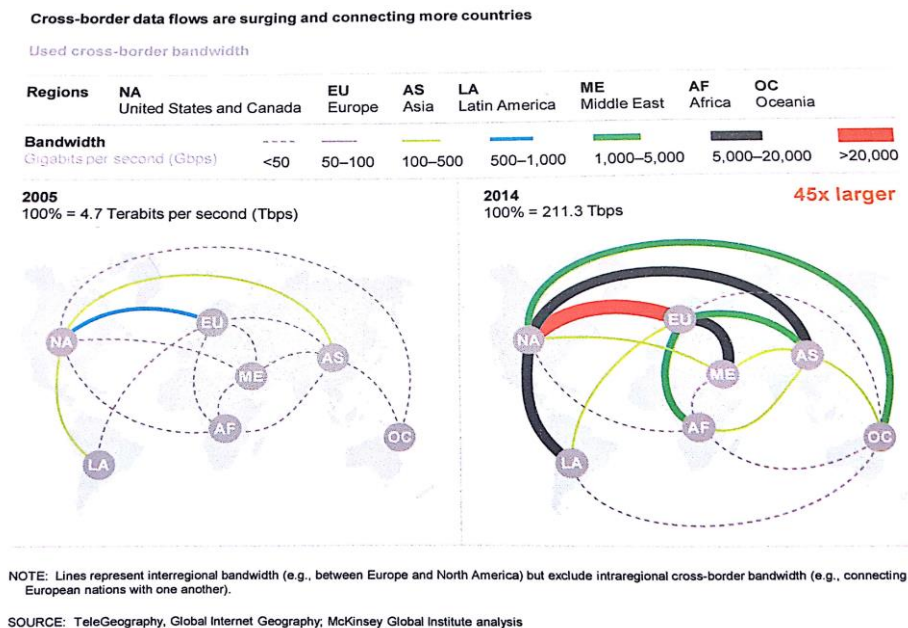
A nova economia²⁰ assenta num novo conjunto de princípios, como a colaboração, a abertura, a partilha, a interdependência, a integridade (nomeadamente, Tapscott, 2015, p. 3; Rifkin, 2016, 37), promovendo a horizontalidade da circulação, a desintermediação dos serviços, a democratização e a distribuição de poder, a co-produção de bens (nomeadamente, Toffler, 1980, p. 251; Rifkin, 2016; Kotler, Kartajaya e Setiawan, 2017, p. 27-39; Schultz, 2013, p. 144; Langley e Leyshon, 2016, 3). Kotler, Kartajaya e Setiawan (2017, p. 27-39) sublinham, ainda, que “a transferência de poder para os consumidores conectados” assenta em três transições: do vertical para o horizontal; do exclusivo para o inclusivo; e, do individual para o social.

Por outro lado, os fluxos digitais que materializam a economia digital estão a alterar, também, a própria estrutura empresarial (Tapscott, 2015, p. 3 e 15 a 22). Podemos ver uma demonstração do aumento exponencial dos fluxos digitais no estudo *Digital Globalization: The New Era of Global Flows* (McKinsey Global Institute, 2016, p. 4) - Figura 1. Por seu turno, no estudo *Data-Driven Transformation: Accelerate At Scale Now* (Boston Consulting Group, 2017, “Exhibit 1”) – Quadro 1 –, vemos como a nova economia provocou a alteração da estrutura empresarial: as empresas mais valiosas são aquelas cujo modelo de negócio se baseia na informação.

²⁰ A nova economia é, para Castells (2002, p. 77-78), informacional, global e em rede.

Figura 1: aumento dos fluxos digitais.

Fonte: Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016




Quadro 1: crescimento empresas de base informacional

Fonte: Data-Driven Transformation: Accelerate At Scale Now (Boston Consulting Group, 2017)

Data-Driven Companies Have Become the Most Valuable

COMPANY: MARKET CAPITALIZATION

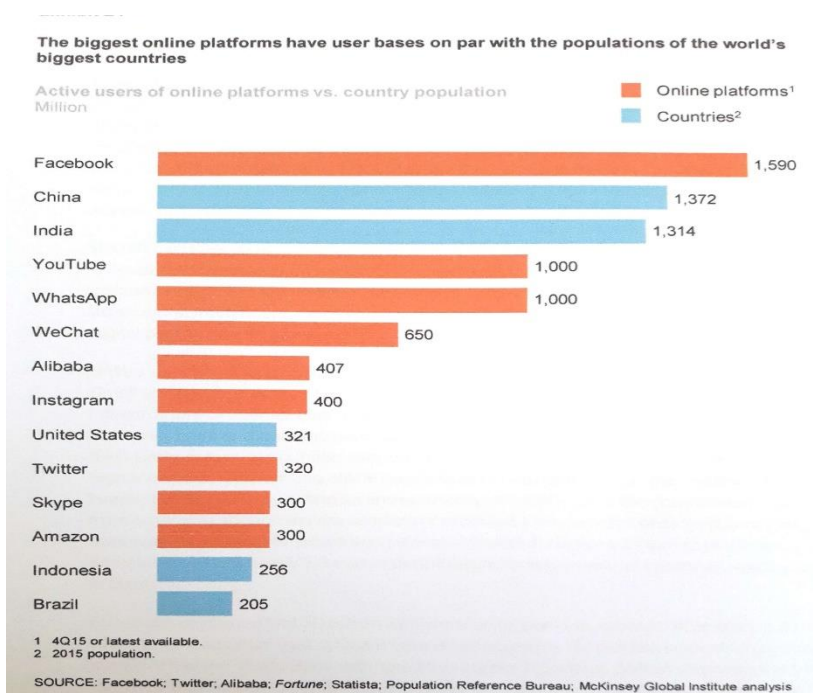
RANK	APRIL 2017	Q4 2011	Q4 2006
1	Apple: 741	Exxon Mobil: 406	Exxon Mobil: 447
2	Alphabet: 585	Apple: 376	General Electric: 384
3	Microsoft: 505	PetroChina: 277	Microsoft: 294
4	Amazon: 432	Royal Dutch Shell: 237	Citigroup: 274
5	Facebook: 408	ICBC: 228	Gazprom: 271
6	Berkshire Hathaway: 404	Microsoft: 218	ICBC: 255
7	Exxon Mobil: 344	IBM: 217	Toyota: 241
8	Johnson & Johnson: 330	Chevron: 212	Bank of America: 240
9	JPMorgan Chase: 303	Walmart: 205	Royal Dutch Shell: 226
10	Alibaba Group: 278	China Mobile: 196	BP: 219

 Data-driven company

Source: S&P Capital IQ, "Top 10 Companies with Highest Market Capitalization Worldwide."
Note: Market capitalization figures have been rounded and are in \$billions.

Por fim, e mais recentemente, o surgimento das plataformas digitais intensificou os impactos sociais e económicos da economia digital (McKinsey, 2016, p. 1-2): alterou a forma de fazer negócio (em virtude da redução custos de interacção e transacção, e do aumento da importância das economias de escala); criou mercados e comunidades de escala global (mais fácil acesso a clientes, a empresas e um aumento da eficiência e rapidez de contacto); permitiram crescimento de pequenas empresas (em virtude do mais fácil acesso aos mercados globais); e permitiu a participação directa dos agentes económicos (particulares) no mundo globalizado (democratizando o ensino, o trabalho, a divulgação pessoal, no que se pode traduzir num aumento de poder). Para a McKinsey (2016, p. 6), as plataformas digitais desempenham um papel chave na nova era da globalização, porque permitem ligar tudo, todos em qualquer sítio. A dimensão destas plataformas é apresentada no Gráfico 2, com referência ao estudo da McKinsey *supra*-referido (2016, p. 6).

Gráfico 2: dimensão plataformas digitais



Fonte: Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016

Parker, Alstynne e Choudary (2016, p. 5-23) consideram que as plataformas digitais encerram uma verdadeira revolução – a Revolução das Plataformas –, em virtude de basearem o seu modelo de negócio na criação de valor através das interações entre produtores e prestadores de serviços e os clientes (Langley e Leyshon, 2016, analisam as plataformas enquanto formas de

intermediação), invertendo (ou reconfigurando) a estrutura das empresas (dão como exemplo, na área financeira, o Bitcoin). As plataformas baseiam-se na informação e na criação de comunidades, razão pela qual, é dada especial atenção aos efeitos de rede na criação de eficiências.

No entanto, Ross (2016, p. 106-107) põe em evidência que,

“Os mercados codificados (...) concentram e dispersam simultaneamente o mercado. Com a disponibilização de mercados codificados mesmo aos mais pequenos fornecedores, surgiu uma tendência que afasta as transacções das lojas físicas ou dos hotéis e na direcção das pessoas individuais, ligando-se localmente ou *online*. É assim que o mercado se dispersa. O trajecto da sua dispersão, no entanto, redirecciona cada uma dessas transacções através de um pequeno número de plataformas tecnológicas sediadas na Califórnia ou na China. É assim que se concentra o mercado.”

É em virtude desta concentração, promovida pelos efeitos de rede e com os ganhos de eficiência, que algumas plataformas (que não deixam de ser empresas) conseguiram quotas de mercado tão significativas.

Por fim, importa sublinhar que a digitalização da economia (e a mudança para uma economia baseada na informação) tem provocado um outro efeito, decorrente da enorme diminuição dos custos de comunicação e dos custos de reprodução de bens digitais: a aproximação a um custo de marginal de produção próximo de zero (Rifkin, 2016, 18; Brynjolfsson e Saunders, 2010, p. xiv), com enorme potencial disruptivo para a sociedade.

2.2. A moeda e o Estado

A invenção da moeda, pelos sumérios, há cerca de 5000 anos, foi um dos mais importantes marcos na história da civilização, tendo permitido o desenvolvimento de estruturas sociais mais complexas, nomeadamente, da organização burocrática de gestão da sociedade (entre outros autores, Ingham, 2004, p. 3; Ingham, 2016, p. 67; Harari, 2017, p. 184-186). Rogoff (2016, p. 17-18), de forma expressiva, descreve esta invenção como um salto quântico na história da civilização. A razão da importância da moeda é, usualmente associada às funções que desempenha na sociedade: em primeiro lugar, é um meio de troca eficiente (permitindo a divisão do trabalho e a troca de bens e serviços de forma simples); em segundo lugar, a moeda funciona como uma reserva abstracta de valor (enquanto poder de compra futuro); por fim, a moeda funciona como unidade de conta (ao permitir, por exemplo, a definição e cálculo de

custos, benefícios e dos preços²¹) (Ingham, 2004, p. 3-4; Samuelson e Nordhaus, 2005, p. 513; Daniel, 2013, p.125).

Apesar da importância da moeda, ou do dinheiro, na organização das sociedades, não existe na teoria económica uma definição unânime do conceito de moeda (Cohen, 1998, 10; Daniel, 2013, p. 125)²², antes surgindo delimitado, habitualmente, por referência às suas funções típicas²³: “permitir a troca de forma prática, sendo a troca directa pouco cómoda; associar cada bem a um preço; conservar no tempo poder de compra, expressão de um valor.” (Daniel, 2013, p.125). Autores como Ingham (2004, p. 3; 2016, p. 67) e Martin (2013, p. 39) encaram a moeda, o dinheiro, como uma tecnologia social.

Ingham (2004, p. 4) destaca, ainda, invocando a obra e terminologia de Mann (autor que estudou a origem do poder social), que a moeda não é apenas poder “poder infraestrutural” mas também “poder despótico”: o poder infraestrutural refere-se às funções da moeda, na organização da sociedade, ao passo que o poder despótico se refere à possibilidade de apropriação da moeda por interesses particulares, como por exemplo, do Estado (esta apropriação não é uma questão de quantidade, de posse, mas de controlo, como é o caso da produção de moeda).

Neste sentido, podemos dizer, conforme refere Ross (2016, p. 111), que “Nada simboliza mais a soberania de um Estado do que a sua moeda. Colocamos fotografias de presidentes, monarcas e primeiros-ministros nas notas bancárias. A moeda está enraizadamente associada à nossa noção de economia nacional, autonomia nacional e mesmo identidade nacional.” Todavia, como refere Cohen (1998, p. 4), o paradigma Um Estado/Uma Moeda é relativamente recente, e deriva das convenções relativas à definição de fronteiras, aquando da instituição da Paz de Vestefália, que pôs fim à Guerra dos 30 anos, no século XVII. O acordo relativamente às fronteiras foi, simultaneamente, uma delimitação geográfica da soberania absoluta de cada Estado, enquanto unidade básica de governação na política mundial. O mesmo autor acrescenta, porém, que só no século XIX é que os Estados começaram a exercer uma maior controlo sobre a criação e a gestão da moeda (o “poder despótico” de Mann), como forma de consolidação do

²¹ O controlo dos preços está, usualmente, associado ao controlo da inflação (subida geral de preços) e da deflação (descida geral de preços). Fisher (2015, p. 46-48) sublinha que “o nível de preços é aumentado ou diminuído (isto é, o poder de compra do dinheiro é diminuído ou aumentado) pela inflação ou deflação *relativas* – pela circulação monetária ultrapassar a circulação de bens, ou o inverso.”

²² O facto de o próprio conceito de moeda não ter uma definição estabilizada na doutrina económica só acrescenta dificuldades quanto ao tratamento conceptual do Bitcoin, quando associado a essa função.

²³ A este respeito, *vide* Fernandes e Mota (2015, p. 13), onde podemos ler que, “Moeda é tudo aquilo que é geralmente aceite como meio de pagamento. Portanto, moeda não é nada de concreto! Não é nada que se identifique com uma forma ou com um qualquer material. Pelo contrário, a moeda define-se em termos funcionais, ou seja, da capacidade de algo para desempenhar aquela função de meio de pagamento geralmente aceite.”

seu poder (moedas territoriais) (*ibidem*, p. 32). Este controlo estava intimamente ligado aos sistemas nacionalistas, e o poder resultante derivava do monopólio monetário, mediante quatro canais: simbolismo político (promotor de unidade), direitos de senhoriagem (e o implícito aumento da oferta monetária, com o objectivo de aumentar a despesa pública), gestão macroeconómica (com impacto na produção interna e no controlo do desemprego; capacidade para regular as taxas de câmbio, em termos de trocas internacionais), e isolamento monetário (independência monetária e aumento da autoridade estatal) (*ibidem*, p. 35-46).

Cohen (1998, p. 4) refere, por outro lado, que o modelo de mercado aberto e de concorrência alterou profundamente a organização espacial das relações monetárias, o que provocou uma erosão no monopólio dos Estados. Este autor (*ibidem*, p. 150) conclui observando que a economia actual, globalizada e interdependente, promoveu o aparecimento de redes impessoais de transação, de troca, que são alheias às fronteiras dos Estados, num mundo ainda marcado pelo princípio das soberanias nacionais, o que provoca uma crise de legitimidade e inúmeras tensões e inseguranças.

O controlo da moeda pelo Estado tem um papel decisivo nas economias modernas. Samuelson e Nordhaus (2005, p. 510) avançam que “o dinheiro tem tudo menos falta de utilidade de um ponto e vista macroeconómico. A política monetária é activamente a mais importante ferramenta que o Estado dispõe para estabilizar o ciclo económico.”²⁴ Importa acrescentar que, além da estabilização do ciclo económico, o controlo da moeda permite ao Estado exercer controlo sobre os fluxos monetários para efeitos fiscais, bem como, para executar a sua política económica e orçamental (Friedman, 2014, p. 71)²⁵.

O papel da moeda (e do seu controlo pelo Estado) adquire maior significado se considerarmos que tanto as economias de troca capitalista como as economias de troca socialista assentam, essencialmente, em trocas realizadas com meios monetários (Nunes e Valério, 2012, p. 62). Porém, estas trocas nem sempre se realizaram no âmbito de sistemas monetários. Na verdade, e como referem Fernandes e Mota (2015, p. 9), “Cronologicamente temos em primeiro lugar as chamadas economias de troca directa que correspondem a um estágio inicial e bastante

²⁴ Por política monetária entende-se “a actuação das autoridades monetárias sobre a quantidade de moeda em circulação, de crédito e das taxas de juros, controlando a liquidez global do sistema económico, que irá afectar a situação macroeconómica. Alguns dos objectivos macroeconómicos típicos, que cabe à política monetária assegurar, são: elevado nível de emprego; crescimento económico; estabilidade de preços; estabilidade das taxas de juros; estabilidade dos mercados financeiros; estabilidade do mercado cambial.” (Silva, 2012, p. 87).

²⁵ Por política orçamental entende-se a “gestão dos recursos do Estado. Os dois principais instrumentos de política orçamental são a despesa pública (gastos) e a receita pública (fundamentalmente, impostos). Uma redução de gastos do Estado leva a uma redução na procura de bens e serviços. Um aumento dos impostos implica uma redução no rendimento disponível dos consumidores, levando a uma diminuição do consumo. Embora os efeitos de uma política orçamental sejam claros e rápidos, a determinação dessa política envolve grandes compromissos.” (Silva, 2012, p. 88).

imperfeito no desenvolvimento das sociedades humanas.” Esta teoria, de que no início o comércio era realizado mediante troca directa (por permuta), foi contestada, entre outros, por Martin (2013, p. 20-24), que evidencia que “Por mais que procurassem, nenhum investigador conseguiu encontrar uma sociedade, histórica ou contemporânea, que realizasse regularmente o seu comércio através da permuta.”, sublinhando, depois, que “Centrar-se no pagamento em espécie e não no sistema de crédito e compensação que existia por detrás dele [do comércio] era ter uma compreensão totalmente errada das coisas.” Na verdade, este autor defende que “a moeda circulante não é, em si mesma, o dinheiro. O dinheiro é o sistema de contas de crédito e a sua compensação representada pela moeda circulante.”

Independentemente destas considerações, e seguindo a teoria convencional, mesmo depois da evolução da economia (e da sociedade) para sistemas monetários, muitas vezes o sistema de troca directa reaparece, por necessidade. Middelkoop (2017, p. 27) selecciona os seguintes eventos, a título de exemplo: a utilização de cigarros como meio de troca durante a Segunda Guerra Mundial; o colapso da Argentina em 2001; e, o fornecimento de petróleo pelo Irão à China e à Índia, em 2013, como resposta ao boicote económico americano e à exclusão do sistema internacional de pagamentos (SWIFT, acrónimo que corresponde a *Society for Worldwide Interbank Financial Telecommunication*).

De acordo com Fernandes e Mota (2015, p.13), “As economias monetárias surgem com a invenção da moeda.”, tendo os sistemas de troca monetários vivido diversas fases, que se podem distinguir em função do padrão monetário utilizado. Apesar de não caber no âmbito deste excursus uma análise da evolução dos padrões monetários, faremos uma breve resenha dos principais momentos.

Assim, começamos por referir o padrão-mercadoria, o qual, segundo Friedman (2014, p. 72), se traduz na “utilização como dinheiro de uma mercadoria como o ouro ou a prata (...)”. Segundo o mesmo Autor, “O principal defeito de um padrão-mercadoria, do ponto de vista da sociedade como um todo, é que o mesmo implica o uso de recursos reais para aumentar o *stock* de moeda.”²⁶, razão pela qual, este padrão “tem sido acompanhado da criação de vários tipos de dinheiro fiduciário, aparentemente convertível no bem monetário em condições preestabelecidas”.²⁷ No âmbito deste padrão, “a moeda vale o que valer o seu conteúdo intrínseco.” (Fernandes e Mota, 2015, p. 23).

Fernandes e Mota (2015, p. 23-34) distinguem os vários momentos do sistema monetário, referindo-se a sistemas não metálicos e a sistemas metálicos (e, dentro destes, aos sistemas

²⁶ Vide, Friedman (2014), p. 72.

²⁷ *Ibidem*.

monometálicos, aos bimetálicos e ao padrão-ouro)²⁸. O abandono do padrão-ouro, em 1971, ditou a evolução dos sistemas monetários metálicos para sistemas puros de papel-moeda (Silva, Mota, Queirós e Pereira, 2013, p. 52-54, e Fernandes e Mota, 2015, p. 34). “Nessa altura, e até hoje, o sistema monetário passa a basear-se exclusivamente no papel-moeda, ou moeda fiduciária, que circula com um valor intrínseco inferior ao seu valor facial e sem qualquer possibilidade de conversão oficial em ouro.”²⁹.

Aqui chegados, importa sublinhar que as políticas monetária e orçamental não representam fins em si mesmos, antes desempenham uma função instrumental relativamente aos fins essenciais do Estado: garantir o bem-estar dos cidadãos, a sua segurança, a melhoria do seu nível de vida, a justiça social, no fundo, o desenvolvimento (em sentido amplo) da sociedade (cfr. Carvalho, 2011, p. 152, para quem, “O Estado tem um papel fundamental no desenvolvimento.”) e a satisfação das necessidades fundamentais dos cidadãos, no já referido ambiente de escassez de recursos³⁰. Neste sentido, Bento (2004, p. 73) refere que “Teoricamente baseado na voluntária abdicção pelos cidadãos de muitos dos seus direitos, transferidos para o soberano em troca de segurança, o Estado converte-se no polo dominante da esfera pública, competindo-lhe assegurar o bem comum da sociedade e preservar a sua existência pública.” A este respeito importa invocar Diniz (2010, p. 40), que refere que “Nunca será demais realçar o facto de que apesar do progresso económico ser um elemento essencial ao progresso de desenvolvimento, por si só, não representa o processo na sua totalidade. Desenvolvimento está para além do processo económico.” Kulkarni e RaJam (1991, *apud* Diniz, 2010, p. 40-41) preconizam a ideia de que o desenvolvimento corresponde a “um esforço articulado e organizado para se dotar a ele próprio das condições e no contexto da sua existência colectiva.” Continuam estes autores, definindo os objectivos que as sociedades pretendem atingir através do processo de desenvolvimento, os quais elencamos de forma resumida: “melhorar o nível de vida de todos os membros da sociedade”; “contribuir para a criação de condições que conduzam ao amor-

²⁸ Vide, também, Silva, Mota, Queirós e Pereira (2013, p. 52-54).

²⁹ Vide, Fernandes e Mota (2015, p. 34).

³⁰ A respeito do papel económico do Estado, Samuelson e Nordhaus (2005, p. 35) apresentam uma descrição ilustrativa: “no mundo real, nenhuma economia está efectivamente de acordo com o mundo ideal de funcionamento da mão invisível. Em vez disso, todas as economias de mercado sofrem as imperfeições que levam a doenças tais como a poluição excessiva, o desemprego e a extremos de riqueza e pobreza. (...) Como desenvolvem os governos as suas funções? Os governos actuam ao exigir que as pessoas paguem impostos, obedeça, às leis e consomem certos bens e serviços colectivos. (...) Os governos numa economia de mercado têm três funções económicas principais: o aumento da eficiência, a promoção da equidade e o estímulo do crescimento e da estabilidade macroeconómicos: 1. O governo aumenta a *eficiência* ao promover a concorrência, ao combater externalidades como a poluição e ao fornecer bens públicos; 2. O governo promove a *equidade* ao usar os impostos e programas de despesa para redistribuir o rendimento a grupos específicos; 3. O governo estimula o *crescimento e a estabilidade macroeconómicos* – reduzindo o desemprego e a inflação enquanto estimula o crescimento económico – através da política orçamental e da regulação monetária.”

próprio das populações”; “alargar o conjunto de oportunidades económicas e sociais”; “assegurar que o processo de desenvolvimento é sustentável tanto do ponto de vista económico como ambiental.”

De outra perspectiva, importa sublinhar que o padrão monetário, utilizado nas sociedades, também foi afectado pela evolução tecnológica, no que Ross (2016, p. 89-90) designa de movimento de “codificação do dinheiro”. O evoluir das sociedades, a sua complexificação, com maior oferta de bens e serviços e populações mais numerosas, foi exigindo a sofisticação do dinheiro, tendo a tecnologia desempenhado um papel central, em virtude da necessidade de produzir, de forma eficiente, moeda genuína e que fosse dificilmente falsificada (Rogoff, 2016, p. 17-19). A natureza física do dinheiro, das moedas, tem evoluído para a desmaterialização, a par da transição para a sociedade da informação e em consequência das inovações tecnológicas Ross (2016, p. 90) destaca algumas comodidades introduzidas pelo sistema financeiro, como por exemplo, o cartão de crédito, as máquinas ATM, os serviços bancários *online*.

O aparecimento do Bitcoin inscreve-se nesta evolução de codificação do dinheiro. No entanto, não sendo uma moeda criada e gerida pelos Estados, coloca inúmeras questões quanto à capacidade de controlo destes. Num cenário (hipotético) em que o Bitcoin se imponha na sociedade, fica difícil perceber como podem os Estados levar a cabo, de forma eficaz, as respectivas políticas monetárias e orçamentais e, com isso, realizar os fins a que se destinam.

Não obstante, impõe-se referir que a ideia de moedas privadas (no sentido de não serem criadas ou geridas pelo Estado), já foi amplamente concebida pela teoria económica, sendo a escola austríaca disso exemplo. É o próprio Banco Central Europeu (2012, p. 22) que faz a ligação entre o Bitcoin e a escola austríaca (de pensamento económico)³¹: “As raízes teóricas do Bitcoin podem ser encontradas na escola austríaca e nas suas críticas ao sistema atual de moeda fiduciária, bem como, relativamente às intervenções realizadas pelos governos e outras entidades que, em sua opinião, resultam em ciclos económicos exacerbados e inflação maciça.”

Segundo o Banco Central Europeu (2012, p. 22), o pensamento da escola austríaca assenta na concepção de que,

“os ciclos económicos são a consequência inevitável de intervenções monetárias no mercado, mediante as quais uma expansão excessiva do crédito bancário causa um aumento da oferta de dinheiro através do processo de criação de dinheiro bancário (sistema de reservas fracionárias), que por sua vez leva a

³¹ De acordo com Boettke, a escola austríaca foi “fundada em 1871 com a publicação dos Princípios de Economia de Carl Menger.” De acordo com o mesmo autor, a verdadeira unidade de análise da teoria económica é o homem e as suas escolhas e que estas “são determinadas por preferências subjetivas individuais”. A lógica subjacente a estas escolhas “é o elemento fundamental para o desenvolvimento de uma teoria económica universalmente válida.”

taxas de juros artificialmente baixas. Nesta situação, os empresários, guiados pela sinalização de taxas de juros distorcidas, embarcam em projectos de investimento excessivamente ambiciosos que não encontram correspondência nas preferências presentes de consumo intertemporal (i.e., decisões de consumo relativas ao curto prazo e ao futuro) dos consumidores. Mais tarde ou mais cedo, este desequilíbrio generalizado deixa de ser sustentável, e leva a uma recessão, durante a qual as empresas precisam de terminar os projectos de investimento falhados (liquidam o investimento), e de readaptar (reestruturar as suas estruturas de produção, de acordo com as preferências intertemporais dos consumidores.”

No seio desta escola de pensamento económico, Hayek (1990, p. 33-36) questiona como foram as pessoas capazes de suportar durante tanto tempo o poder exclusivo dos governos, que tem sido usado para as explorar e defraudar. Para este autor, a história pode ser vista como inflação criada pelos governos, numa constante distorção da economia, que só foi possível pelo monopólio da moeda. Por conseguinte, Hayek (1990, p. 131-133) apresenta um programa, assente num “Movimento de Moeda Livre comparável ao Movimento de Comércio Livre do século XIX.”, e que pressupõe a existência de um mercado concorrencial de moedas, geridas por privados.

2.3. A crise financeira de 2008 e a regulação bancária

Convém começarmos por frisar que a associação entre o Bitcoin e a crise financeira é feita pelo próprio criador, Nakamoto, o qual, aquando da criação do Bloco Génesis, publicou a seguinte mensagem: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks” – uma referência directa aos resgates bancários com dinheiros públicos. Conforme refere Ulrich (2014, p. 43),

“A alusão à manchete do jornal britânico *The Times* daquele dia não é accidental. É, na verdade, um claro indicativo da visão crítica de Satoshi [Nakamoto] sobre o sistema bancário e a desordem financeira reinante. (...) o projecto Bitcoin vinha a ser uma tentativa de resposta à instabilidade financeira causada por décadas de monopólio estatal da moeda e por um sistema bancário de reservas fracionárias.”

Por conseguinte, parece-nos que a compreensão cabal do fenómeno Bitcoin convoca um entendimento, ainda que breve, dos contornos da crise financeira. Neste ensejo, e segundo o ensinamento de Carvalho (2014, p. 59), que subscrevemos na íntegra, cumpre mencionar que,

“A primeira década do século XXI termina com um ciclo de profundas perturbações e transformações das economias e das sociedades à escala global. Acumula duas relevantes recessões (2001-2003 e 2008-

2009) e uma crise económica e financeira que marcará, pelo menos, a primeira metade da segunda década enquanto “palco” de uma lenta e complexa reestruturação dos modelos de organização das empresas, das fontes de criação de riqueza, das formas de regulação dos mercados, dos critérios de condução das políticas económicas e dos níveis e áreas de proteção social.”

Carvalho (2011, p. 37) reconhece, a respeito da crise de 2008, que a atenção dos analistas e investigadores se tem focado, primordialmente, “na crise financeira centrada no sistema bancário”, mas considera, adicionalmente, que “A «tempestade» foi alimentada por um conjunto de outros factores que promoveu um grave choque de preços: um brusco aumento nos preços da energia, das matérias-primas e dos géneros alimentares.”

Para Gamble (2009, p. 13-35), o caminho que levou às crises de 2000 e de 2008 foi longo, e resulta do *boom* dos anos 80 e 90 e da adopção de um novo modelo de crescimento, apoiado nas doutrinas monetaristas³² e da economia pelo lado da oferta³³. Este novo modelo de crescimento teve como condições essenciais, à sua plena implementação, a desregulação dos mercados financeiros (anos 80 e 90) – a qual promoveu um capitalismo de casino, com foco no curto prazo, e alavancada em dívida cujos riscos eram depois “socializados” pelo sector bancário –, e a emergência económica da China, Índia, Brasil e outros países – o que permitiu o controlo da inflação, através do fornecimento de produtos mais baratos, consequência de uma mão-de-obra também ela mais barata. Refere o mesmo autor (Gamble, 2009, p. 13-35), que este modelo promoveu o aparecimento de várias bolhas especulativas, sendo as mais graves a bolha das “dot.com” (crise de 2000), e a bolha do mercado imobiliário (crise de 2008).

No que tange a crise de 2008 especificamente, Valdez e Molyneux (2010, p. 304-306) distinguem, com referência ao *Global Financial Stability Report*, do FMI, de 2009, as causas macroeconómicas das microeconómicas. Quanto às primeiras, referem o acumular de desequilíbrios financeiros globais e as taxas de juro baixas (taxas que levaram a um *boom* de crédito, em especial, nos empréstimos hipotecários). Quanto às segundas, referem o desconhecimento dos riscos pelos consumidores, a orientação para os lucros de curto prazo pelos gerentes das empresas financeiras, obtidos com suporte em alavancagem financeira, a política de remunerações incentivadora da tomada de riscos, os distorcidos e desalinhados

³² Relativamente ao monetarismo, e de forma resumida, podemos dizer que se trata de uma escola do pensamento económico que defende que a oferta de moeda é um dos principais determinantes do crescimento do produto nacional, sendo os instrumentos monetários a principal ferramenta para manter a estabilidade da economia (McCallum, n/d).

³³ No que respeita a economia pelo lado da oferta, trata-se de uma corrente económica que defende que a oferta estimula a procura, e de que altas taxas de imposto desencorajam a criação de riqueza e de eficiência. De acordo com esta corrente económica, a redução dos impostos não implica uma diminuição da despesa pública, porquanto a poupança fiscal (atribuída aos privados) é reinvestida na economia, levando a um aumento da receita fiscal (Gwartney, n/d).

incentivos das agências de *rating*, e as graves limitações na análise de risco, na sua gestão e na respectiva supervisão regulatória. Referem, também, que uma das principais causas da crise de 2008 se ficou a dever ao fenómeno da “securitização”, ou seja, da transformação de créditos bancários em produtos financeiros (“investimentos”), como forma de diluição dos riscos inerentes a esses mesmos créditos (*verbi gratia*, risco de incumprimento).

McMillan (2014, 54-55) sublinha que as tecnologias de informação e de comunicação, particularmente desde os anos 70 do século XX, transformaram o sector bancário, tendo permitido aos bancos elaborar estruturas de contabilidade complexas: “mobilizaram o crédito”. Para este autor, se os bancos eram resistentes a complexificar as suas estruturas antes da revolução digital, o advento de novas tecnologias permitiu aos bancos, com grande facilidade e eficiência, criar estruturas que permitiam contornar os controlos das entidades reguladoras. No fundo, como refere o autor, permitiu o *shadow banking*. Um dos instrumentos do *shadow banking* foi a já referida securitização de créditos, os quais eram posteriormente movimentados através de *special purpose vehicles*, que, por sua vez, criavam outros produtos financeiros, para apresentar ao mercado (v.g., os designados *asset-backed securities*), e, assim, socializar o risco (mas não o proveito) (McMillan, 2016, 65-78). O sucesso destas técnicas assentava numa profunda assimetria de informação.

Além dos graves efeitos sociais e humanos, muitas instituições financeiras faliram, acentuando a degradação da confiança económica. A resposta dos governos passou, maioritariamente, por medidas de recapitalização de bancos através do *quantitative easing*, claro está, à custa dos orçamentos e dívida públicos, muitas vezes sob o argumento de que as instituições financeiras em causa eram demasiado grandes para falir (*too big to fail*) – o que estimulou, mais ainda, a propensão para concessão de crédito de risco (*moral hazard*) (McMillan, 2016, 97-100).

Carvalho (2011, p. 50) refere, expressivamente, que “A principal preocupação deriva dos efeitos colaterais do remédio utilizado para impedir o colapso do sistema financeiro internacional. O remédio foi utilizar montanhas de dinheiro para não secar o crédito.”

Ora, o paradigma económico capitalista assenta precisamente sobre o binómio crédito-dívida³⁴, e também sobre a circulação do dinheiro, razão pela qual, atenuar os efeitos do *credit crunch* era tão importante. “Desde 2007, a Reserva Federal Americana (FED), o Banco Central Europeu (BCE), o Banco de Inglaterra e o Banco do Japão recorreram ao Quantitative Easing (QE) para injectar mais de US\$ 4 biliões na liquidez adicional das suas economias.” (Carvalho,

³⁴ Cfr., a este respeito, Carvalho (2011, p. 194), onde lemos o seguinte: “Para Schumpeter, o crédito, e não a acumulação de capital, era essencial para o desenvolvimento, na medida em que permitiria aos empresários – os indivíduos com a função de realizar combinações novas dos factores produtivos – obter poder de compra para efectuar as combinações novas que não podem ser financiadas pelos lucros de produções anteriores.”

2014, p. 92). Estas injeções de capital, financiadas com os impostos dos cidadãos, permitiram a muitos bancos (os que não faliram) limpar os seus activos tóxicos (socializando, outra vez, mas por outro meio, os riscos). O mesmo é dizer, que as graves consequências do comportamento (“irregular”?) dos bancos, e de outros intervenientes do mercado financeiro, foi aplacado à custa dos principais prejudicados: os cidadãos – considere-se, em particular, o caso da crise cipriota, em 2013, em que foram “confiscadas” poupanças de depositários (o que originou uma corrida aos bitcoins, e uma apreciação significativa do respectivo valor).

Além das injeções de capital, a resposta governativa implicou, também, um aumento de regulação e de supervisão do sector financeiro (McMillan, 2016, p. 98-99). Com efeito, os governos e as entidades reguladoras “perceberam” que o sector financeiro era marcado por sistemas de governação e de gestão de riscos desadequados, e por um desalinhamento da estrutura de incentivos, que propiciava a concessão de crédito não sustentável (de risco), tendo levado à instituição de “novas regras de capital mínimo em relação à sua qualidade, liquidez e absorção de prejuízos, com o objetivo de reforçar a estabilidade e o crescimento do sistema financeiro a nível mundial.” (Mendes, 2013, p. 20).

Estas regras resultam do acordo conseguido em 2010, conhecido como Basileia III. “Este acordo vem aumentar as exigências de capital nos bancos com o objetivo de melhorar a sua qualidade e de alargar a capacidade dos mesmos para absorverem perdas e resistirem aos momentos com alguma escassez de liquidez. Exigiu também a introdução de novos requisitos regulamentares sobre a liquidez bancária e alavancagem”. (Mendes, 2013, p. 20).

Considerando o exposto, percebe-se que o fenómeno Bitcoin possa ser encarado como uma contracultura, que acredita na insustentabilidade do actual sistema financeiro e que enfatiza a injustiça que subjaz às soluções governativas adoptadas perante uma crise provocada pelos líderes desse sistema (Vigna e Casey, 2016, p. 13). Referem estes autores, ainda, que o Bitcoin ofereceu uma alternativa ao sistema financeiro vigente, que estava em colapso e que ameaçava arrastar consigo biliões de pessoas.

A regulação bancária, com a qual se pretende controlar os riscos da respectiva actividade, tem sido causa de enormes custos para os bancos (*verbi gratia*, de organização e reporte de informação). Além disso, importa referir também que o sistema financeiro enfrenta, hoje em dia, novos concorrentes (além das tecnologias baseadas na tecnologia Blockchain).

De acordo com Alt e Puschmann (2012, p. 204), a indústria bancária foi das indústrias pioneiras na adopção de tecnologias de informação, facto que resulta, em grande medida, de o negócio bancário ser, essencialmente, um negócio de informação, que pode ser realizado, precisamente,

com o suporte dessas mesmas tecnologias. No entanto, o próprio mercado digital é fonte de profundas transformações neste sector.

Alt e Puschmann (2012, p. 204-205) defendem a existência de 4 motores de transformação do sector bancário: o primeiro prende-se com as consequências da crise financeira (económicas e regulatórias); o segundo versa as alterações de comportamento dos consumidores bancários (com o aparecimento dos *digital natives*), que muitas vezes procuram serviços que se encontram fora do escopo da banca tradicional (por exemplo, pagamentos móveis, *crowd funding*, entre outros); em terceiro lugar, o ritmo de difusão das inovações no âmbito das tecnologias de informação e comunicação, que encerram o potencial de alterarem a relação consumidor-fornecedor; por fim, o aparecimento de *non-banks*, entidades não bancárias que prestam serviços inovadores concorrentes dos serviços tradicionais bancários, e que põem em crise a integração vertical da cadeia de valor bancária³⁵.

Alt e Puschmann (2012, p. 212-213) sublinham que estas tendências promovem enorme pressão sobre os Bancos, e que existe um risco sério de desintermediação, provocada, essencialmente, pelas instituições não bancárias e outros novos actores, consequência do aparecimento de novas soluções tecnológicas. A este respeito, referem o seguinte:

“Discutido intensamente na literatura sobre mercados eletrónicos (por exemplo, Malone *et al.*, 1987) (Benjamin e Wigand 1995), (Giaglis *et al.*, 2002), (Glassberg e Merhout, 2007)), a desintermediação sugere que, ao reduzir os custos de transação e de coordenação, em geral, passam a ser viáveis mais padrões de coordenação intensiva e que os mercados eletrónicos podem substituir os intermediários existentes.”

Arvidsson (2014, p. 462-463) argumenta que o campo dos pagamentos³⁶ vive enorme turbulência na Europa, causada pela incerteza quanto à forma como os pagamentos se processarão no futuro. Refere que os potenciais ganhos residem na substituição da moeda física por moeda electrónica, na mesma linha de Rogoff (2016).

2.4. O fenómeno da confiança

³⁵ Também neste sentido, Arvidsson (2014, p. 465), cita um estudo levado a cabo pelo Sveriges Riksbank, em 2013, onde se conclui o seguinte: “the industry is now facing increased fragmentarization via an increase in payment services provided by an increased number of actors based on new technologies and technological systems. This means that different consumers and merchants must make more choices where not only technologies but also the underlying financial services differ significantly. It will be increasingly difficult to make choices and system risks may increase.”

³⁶ Para Arvidsson (2014, p. 463), o campo dos pagamentos engloba, por um lado, o sistema de pagamentos, e, por outro, o ambiente que envolve o sistema de pagamentos (incluindo-se aqui os valores sociais, factores económicos, questões políticas, evolução tecnológica, questões ecológicas e legais).

A já referida aceleração da sociedade, provocada pelo progresso tecnológico, é analisada por Innerarity (2011, p. 36-38) sob três prismas: aceleração técnica, aceleração da mudança social, e aceleração do ritmo vital. Segundo o mesmo autor, esta aceleração propiciou “uma cultura do presente absoluto sem profundidade temporal. A origem desta relação com o tempo encontra-se na aliança estabelecida entre a lógica do lucro imediato, própria dos mercados financeiros, e a instantaneidade dos meios de comunicação.” (*ibidem*, p. 35). Este imediatismo, a “cultura da urgência”, reduz a capacidade de as sociedades fazerem planos a longo prazo, transformando a política em demagogia (*ibidem*, p. 40-43; Han, 2016, p. 29). Neste seguimento, Innerarity (2011, p. 140) defende que “Se examinarmos a nossa actual relação com o futuro, o trato que as democracias ocidentais mantêm com o provir, teremos de concluir, a meu ver, que, apesar de toda a nossa liturgia da novidade e das diversas retóricas da ilusão, o começo do século XXI se recorta actualmente sobre um fundo de radical desconfiança.”

Sucedem que, como refere Finuras (2013, p. 25), “A confiança é um problema central na existência humana. (...) os «animais humanos» são dotados de uma necessidade instintiva de cooperação e confiam nos outros de forma a conseguirem satisfazer as necessidades mais básicas do ponto de vista emocional, psicológico e material, para fazerem face às necessidades de preservação, sobrevivência, adaptação e reprodução alargada.”

É em virtude desta necessidade que se reconhece que “O homem é um ser complexo, cuja existência se define pela forma como resolve as tensões da sua dúplice dualidade”: a primeira interna (matéria – espírito); a segunda externa (individualidade – comunhão) (Bento, 2004, 11-12). Acrescenta Bento (*ibidem*, p. 12) que, o homem “procura, através dessa comunhão, não só a concretização da sua natureza humana, mas também, de certo modo, transcender a sua finitude e mortalidade, integrando-se num todo colectivo”.

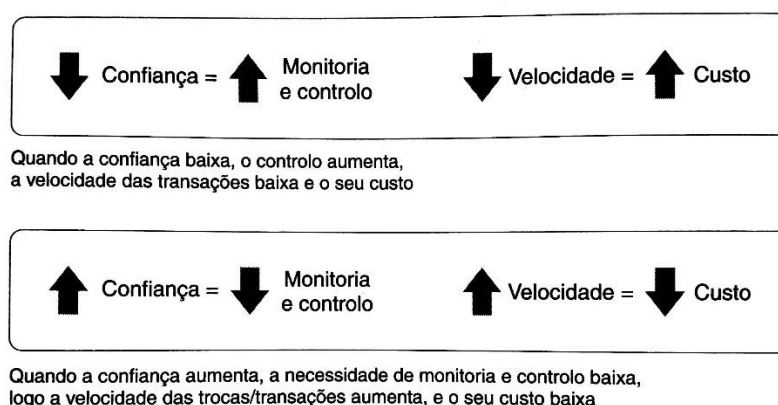
Podemos dizer, considerando a já referida teoria da acção humana de Maslow, que os seres humanos se organizam em sociedades para, em conjunto, colaborando uns com os outros, satisfazerem as suas necessidades. Para Bento (2004, p. 21), o bem comum resultante da agregação dos membros da sociedade depende “da qualidade das inter-relações sociais, dos padrões de reciprocidade e, particularmente, dos níveis de confiança mútua estabelecidos entre os membros da sociedade.” Finuras (2013, p. 35) refere que “a confiança remete para a coesão social, considerada indispensável ao funcionamento das sociedades modernas, complexas e diferenciadas”.

Por outro lado, e de um ponto de vista económico, autores como Putnam, Uslaner e Fukuyama sublinham o papel essencial que a confiança desempenha na promoção do crescimento

económico e no desenvolvimento (Finuras, 2013, p. 35). Acresce que, “a confiança aumenta a previsibilidade positiva, e isso tem um impacto também positivo não só na criação de riqueza numa sociedade, como na própria rapidez das suas interações e no chamado «custo das transacções»”(Finuras, 2013, p. 138). Finuras (2013, p. 139-143) acrescenta ainda que, “Quando não há confiança, cada um tende a passar mais tempo a proteger-se do que a cumprir a sua função e as expectativas a ela associada. Esses comportamentos, quando se generalizam e persistem, tornam qualquer mercado, instituição ou sociedade, menos eficiente”: menos confiança exige mais monitoria e controlo (que engloba o custo da informação), e diminui a velocidade das transacções, aumentando o seu custo. No Quadro 2, Finuras (2013, p. 142), esquematiza o impacto da confiança na economia e nas transacções:

Quadro 2: impacto da confiança na economia e nas transacções

Fonte: Finuras, 2013



Os níveis de confiança na sociedade oscilam em função do comportamento dos governantes, das instituições, das decisões tomadas por outros membros da sociedade, entre outros aspectos. A este respeito, Bento (2004, p. 25-26) refere que “A capacidade de representar a sociedade, como um todo, exige que o dirigente consiga estabelecer uma eficaz relação de confiança, ou um outro elo afectivo, com os outros membros da sociedade, o que depende normalmente do funcionamento de apropriadas instituições mediadoras”.

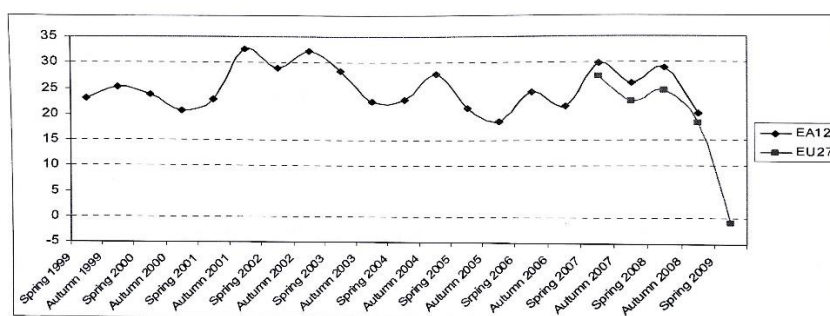
No âmbito do sector financeiro, e especialmente das transacções económicas, o problema da confiança tem sido resolvido mediante a intermediação realizada pelos bancos (e outras instituições financeiras), entre indivíduos e empresas (que não se conhecem), intermediação esta suportada por Bancos Centrais e Entidades Reguladoras, que conferem confiança ao sistema através da supervisão (Adriano e Monroe, 2016, p. 46).

Todavia, recentemente, a crise financeira de 2008 afectou a confiança das pessoas nas instituições financeiras, nas entidades reguladoras e nos próprios governos. Tonkiss (2009, p. 196), Roth (2009, p. 1), Walti (2012, p. 2), entre outros autores, abordam especificamente o decréscimo de confiança decorrente da crise financeira.

Focando-se no caso europeu, Roth (2009, p. 2) refere que o colapso do sistema financeiro tornou os cidadãos europeus conscientes da fragilidade do sistema capitalista, e apresenta dados relativos à confiança em três instituições: no Banco Central Europeu (Gráfico 3); na Comissão Europeia (Gráfico 4); e no Parlamento Europeu (Gráfico 5):

Gráfico 3: evolução da confiança no Banco Central Europeu

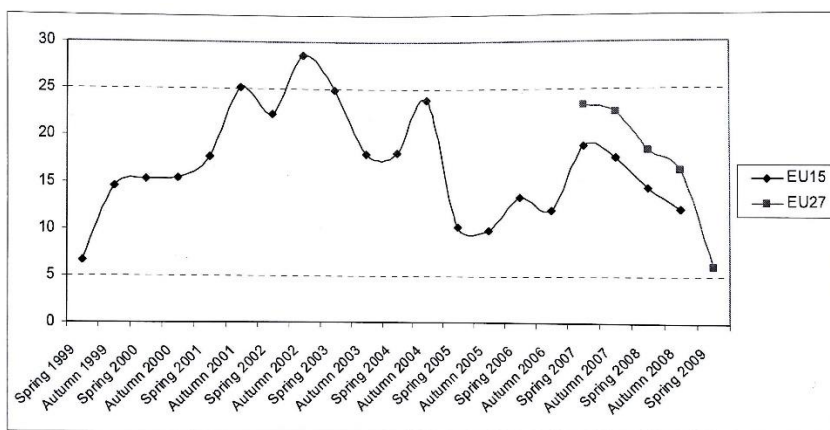
Fonte: Roth, 2009



Data source: Eurobarometer, Standard EB Nos. 51-71

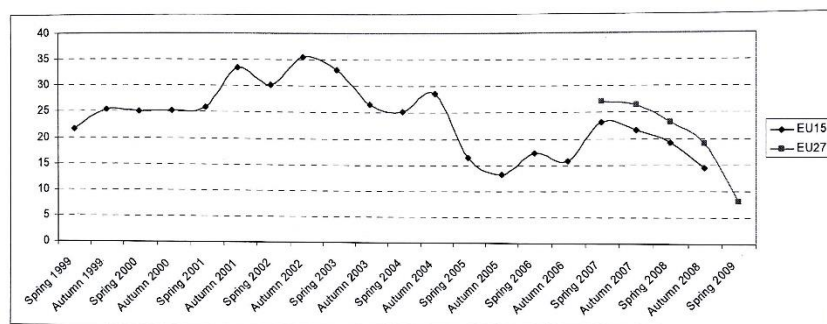
Gráfico 4: evolução da confiança na Comissão Europeia

Fonte: Roth, 2009



Data source: Eurobarometer, Standard EB Nos. 51-71.

Gráfico 5: evolução da confiança no Parlamento Europeu



Data source: Eurobarometer, Standard EB Nos. 51-71.

De acordo com o *2017 Edelman Trust Barometer*, a confiança no sector dos serviços financeiros estava nos 43%, numa base global. Em 2016, a confiança global no sector subiu para os 51%, Apesar da subida, o sector dos serviços financeiros continua a ser o sector que regista os níveis de confiança mais baixos. No Quadro 3, o referido estudo apresenta os níveis de confiança no sector dos serviços financeiros, por país.

Quadro 3: confiança no sector financeiro

Fonte: 2017 Edelman Trust Barometer



É curioso verificar que entre os países mais desconfiados relativamente ao sector se encontram, maioritariamente, países europeus, onde a crise financeira de 2008 foi particularmente violenta.

É neste enquadramento que a tecnologia Bitcoin aparece, pretendendo, na sua essência, substituir a confiança dependente de intermediários (financeiros), por uma confiança “digital”, inerente ao código criptográfico. Neste sentido, Ross (2016, p. 114) refere que,

“o seu método de estabelecer uma genuína inovação na confiança digital, é uma invenção criptográfica chamada *blockchain*. No seu âmago, o *blockchain* é o grande livro-razão em que todas as transacções são registadas. E *absolutamente todas* as transacções, desde o primeiríssimo pagamento em *bitcoins*, ficam registadas no *blockchain*, apesar de o serem anónima ou pseudoanónima.”

Parafraseando Antonopoulos (2015, p. 15), cabe referir que o sistema Bitcoin, ao contrário dos tradicionais sistemas bancário e de pagamentos, se baseia numa confiança descentralizada (ou seja, não resulta da intervenção de uma autoridade central): a confiança do sistema Bitcoin resulta das próprias interacções dos vários intervenientes, ao executarem o código criptográfico. Importa recordar que o Nakamoto (2008, p. 1) considerava que o Bitcoin podia ser uma forma de resolver o actual problema de confiança que afecta a sociedade, levando Tapscott (2016, p. 6), como já referimos, a qualificá-lo como o “Protocolo da Confiança”.

No próximo capítulo, dedicado ao Bitcoin, tentaremos apresentar as características principais desta tecnologia.

3. BITCOIN

Como referimos na Introdução, Nakamoto (2008, p. 1) descreve o Bitcoin como um sistema de pagamentos, no qual é utilizada uma unidade de conta denominada bitcoin. Ou seja, há dois aspectos fundamentais na tecnologia Bitcoin: um, refere-se ao sistema de pagamentos; o outro, à unidade de conta – a moeda. Ou seja, tem uma natureza dual (destacamos Tasca, 2016; Brito e Castillo, 2016, p. 7). A tecnologia Bitcoin é um novo tipo de moeda digital, que circula numa plataforma própria (Tasca, 2016, p. 68). Para Tapscott (2016), o advento da tecnologia Blockchain permite transformar a Web da Informação numa Web do Valor, e que isso poderá trazer nova prosperidade, que assenta, entre outros, nos seguintes pilares: criação de redes *peer-to-peer* assentes em plataformas, promotoras da partilha e da colaboração; alteração do paradigma financeiro, em nome da inclusão e da velocidade de execução e de acesso; protecção de direitos de forma globalizada; eliminação de burocracias e de corrupção (nomeadamente, na ajuda externa a países pobres); valorização do trabalho dos criadores (direitos de autor); reconfiguração do conceito de empresa enquanto motor do capitalismo (predomínio das plataformas); alteração das formas de governação.

Antes de abordarmos estes aspectos, faremos uma breve resenha histórica, relativa aos antecedentes do Bitcoin.

3.1. Antecedentes do Bitcoin

O Bitcoin, enquanto fenómeno tecnológico, não apareceu de forma espontânea, tendo agregado algumas tecnologias preexistentes, e aproveitou o conhecimento gerado pelos anteriores insucessos (Narayanan *et al*, 2016, ix; Rothstein – New Scientist, 2017, p. 23; Carboni, 2017, p. 37). Em virtude deste facto, Antonopoulos (2015, p. 1) considera o Bitcoin “uma coleção de conceitos e de tecnologias que formam a base do ecossistema do dinheiro digital.”. Mougayar (2016, p. 10) encara esta nova tecnologia da seguinte forma: “O blockchain é uma meta tecnologia porque afecta outras tecnologias, e também porque é feita, ela própria, de várias tecnologias. É uma sobreposição de computadores e redes, criados sobre a internet.”

Uma das ferramentas/tecnologias preexistentes foi a criptografia digital, mediante a qual, é possível manter determinada informação privada, em ambiente público (*online*) (Rothstein – New Scientist, 2017, p. 23). Esta tecnologia foi desenvolvida no seio do movimento *cypherpunk* dos anos 90, movimento que tinha como objectivo providenciar formas de garantir a

privacidade na internet (Narayanan *et al*, 2016, 175; Rothstein – New Scientist, 2017, p. 24-26; Vigna e Casey, 2016, p. 42), contornando, mediante ferramentas de encriptação matemática (a criptografia), a vigilância do Estado – o *Big Brother*. Pretendiam anonimato e liberdade na internet, “longe” do controlo do Estado. Este movimento acreditava que, com a privacidade *online* e com criptografia forte, poderia mudar a forma de interacção na internet (Narayanan *et al*, 2016, 175).

Outra ferramenta desenvolvida por este movimento foi a encriptação assimétrica, que permite a duas pessoas comunicarem secretamente, em público (leia-se, na *internet*), sem necessitarem de trocar cifras de desencriptação (Rothstein – New Scientist, 2017, p. 25). A encriptação assimétrica baseia-se na ideia de assinatura digital, realizada mediante “dois objectos digitais: a chave pública e a chave privada.”: uma serve para encriptar uma mensagem, a outra, para realizar o processo inverso (Carboni, 2017, p. 38).

No entanto, Rothstein – New Scientist (2017, p. 27-29) refere também que o movimento *cypherpunk* é apenas metade da história, e que a outra metade nos remete para o mundo das instituições americanas de inteligência e espionagem, que desenvolveram, nos anos 90, o conceito de *onion routing*. Este *software* (TOR ou *The onion router*) permite criar uma rede anónima, em que a identificação de cada computador (do IP ou *internet protocol*) é mascarada e misturada com outras, em diversas camadas de encriptação (a analogia da cebola refere-se, precisamente, a esta várias camadas, que impedem a identificação do endereço dos computadores). Através da rede TOR é impossível descobrir quem envia e quem recebe determinada informação.

Vigna e Casey (2016, p. 42) sublinham que o Bitcoin não foi a primeira experiência de dinheiro virtual ou digital, e que parecia destinado ao mesmo insucesso das anteriores tentativas, na medida em que se baseava nas mesmas ideias e nas mesmas tecnologias: em primeiro lugar, o recurso a encriptação assimétrica para permitir o anonimato; depois, a definição de “regras invioláveis mediante as quais uma rede descentralizada de computadores colaboraria na manutenção da integridade monetária do sistema” (*ibidem*, p. 43.); em terceiro lugar, o acesso livre ao sistema por qualquer pessoa; por fim, tinha o mesmo objectivo, que passava pela substituição dos sistemas de pagamentos e de emissão de moeda, por um outro, em que os privados assumiriam a responsabilidade da sua gestão, mediante códigos matemáticos e recursos computacionais.

Assim, podemos dizer que o Bitcoin é resultado das experiências anteriores, e do conhecimento que o seu falhanço permitiu recolher. Das várias tentativas, destacamos as seguintes: *DigiCash*

(David Chaum, 1989), *hashcash* (Adam Back, 1997), *hashcash* (Adam Back, 1997), *b-monney* (Wei Dai, 1998), *bit-gold* (Nick Szabo, 1998-2005) (Narayanan *et al*, 2016, p. xiii-xxiii).

Um dos principais problemas que estas experiências anteriores enfrentaram foi o do gasto-duplo (*double-spending*): prevenir que a mesma moeda não é utilizada várias vezes (contrafacção). Foi este problema que o Bitcoin, mediante a tecnologia Blockchain, veio resolver (Brito e Castillo, 2016, p. 6).

3.2. O sistema de pagamentos Bitcoin

Relativamente ao Bitcoin, enquanto sistema de pagamentos, importa sublinhar que o mesmo não é controlado por Estados, por bancos centrais, por entidades governamentais, ou mesmo por bancos ou outras instituições financeiras (Rothstein – New Scientist, 2017, p. 3) Aliás, não existe um ponto centralizado de operações neste sistema, sendo antes desenvolvido numa rede descentralizada de computadores, que utilizam um *software* específico para resolver puzzles criptográficos (Nakamoto, 2008, p. 1).

De acordo com Nakamoto (2008, p. 1-7), e de forma sucinta, o sistema Bitcoin consiste numa rede *peer-to-peer*, que permite a realização de pagamentos *online*, directamente entre as partes, sem necessidade de recorrer a intermediários (instituições financeiras), que atestem a validade e legitimidade da transacção. Por outro lado, também não são necessários quaisquer “intermediários de confiança” (instituições financeiras) para resolver o problema do gasto duplo (*double-spending*), porquanto este é evitado através da existência da própria rede *peer-to-peer*. As transacções são adicionadas aos blocos através de funções *hash* (criptografia), depois de resolvido o puzzle matemático (operação criptográfica denominada *proof-of-work*), para a criação de cada bloco de transacções. Este puzzle é de difícil solução mas de fácil verificação pelo resto da rede. Os blocos de transacções vão sendo adicionados a uma corrente de blocos, onde constam todas as transacções já realizadas no sistema (desde o seu início, ou seja, desde o bloco génese) – esta corrente de blocos designa-se Blockchain. Por fim, a segurança da rede (do sistema) exige que pelo menos 51% da rede seja honesta.

Para Mougayar (2016, p. 3-4) as características essenciais do sistema são as seguintes: transacções e interacções electrónicas *peer-to-peer*; ausência de instituições financeiras; prova criptográfica em vez de confiança centralizada; e, confiança na rede em vez de confiança em instituições financeiras. Em função destas características, defende o mesmo autor que sistema Bitcoin, e o Blockchain que lhe subjaz, pode ser visto por três prismas: um prisma técnico, materializando-se numa base de dados que mantém um livro-razão (*ledger*), de forma aberta e

distribuída; um prisma empresarial, por consistir numa rede de trocas, que permite movimentar valor entre os utilizadores; por fim, um prisma legal, em virtude de se tratar de um mecanismo de realização e validação de transacções, que não necessita de intermediários.

Tapscott (2016, p. 29-51), focando-se no Blockchain, sustenta que esta nova tecnologia encerra o poder de revolucionar a forma como organizamos a sociedade³⁷. São sete os princípios de arquitectura que elenca: integridade da rede; poder distribuído; valor como incentivo; segurança; privacidade; garantia de respeito e reconhecimento de direitos; inclusão.

A rede *peer-to-peer*:

Antanopoulos (2014, p. 137) sublinha o facto de o termo *peer-to-peer* significar que os computadores intervenientes no sistema serem pares uns dos outros, ou seja, são todos iguais, com as mesmas responsabilidades, não havendo nós (pontos de ligação do sistema, ou seja, os pares) com premissas especiais. Neste sentido, refere o mesmo autor que os nós do sistema Bitcoin estão interconectados numa rede em malha (*mesh networks*), com uma topologia plana (*flat*), ou seja, estão em pé de igualdade; acrescenta, ainda, que não existe um servidor centralizado, serviços centralizados ou hierarquia dentro da rede, e que os nós consomem e prestam serviços simultaneamente, em reciprocidade, decorrendo daqui a natureza descentralizada, aberta e também a própria segurança. Para Antonopolous (*ibidem*), a descentralização é um princípio essencial da arquitectura do sistema Bitcoin, e que tal descentralização só pode ser assegurada mediante uma rede *peer-to-peer* descentralizada e baseada em consenso maioritário.

Por outro lado, e seguindo novamente Antonopolous (2014, p. 137-138), deve distinguir-se o conceito de “rede Bitcoin” (*Bitcoin network*) – que engloba todos os nós que utilizem o protocolo Bitcoin P2P –, da “rede Bitcoin alargada” (*extended Bitcoin network*) – que engloba outros protocolos, como por exemplo o *Stratum* (utilizado na mineração e em carteiras móveis). Cumpre referir que os nós podem desempenhar diferentes funções, como resulta do Quadro 4. Na Figura 2 encontramos uma demonstração da “rede alargada” de Antonopoulos (2014, p. 140):

³⁷ Como vimos, Tapscott (2016, p.) encara o Blockchain como o “Protocolo da Confiança”, uma vez que a sua arquitectura permite criar confiança sem intermediários, e através de código matemático e informático.

Quadro 4: tipologia dos nós do sistema Bitcoin

Fonte: Antonopoulos (2014)

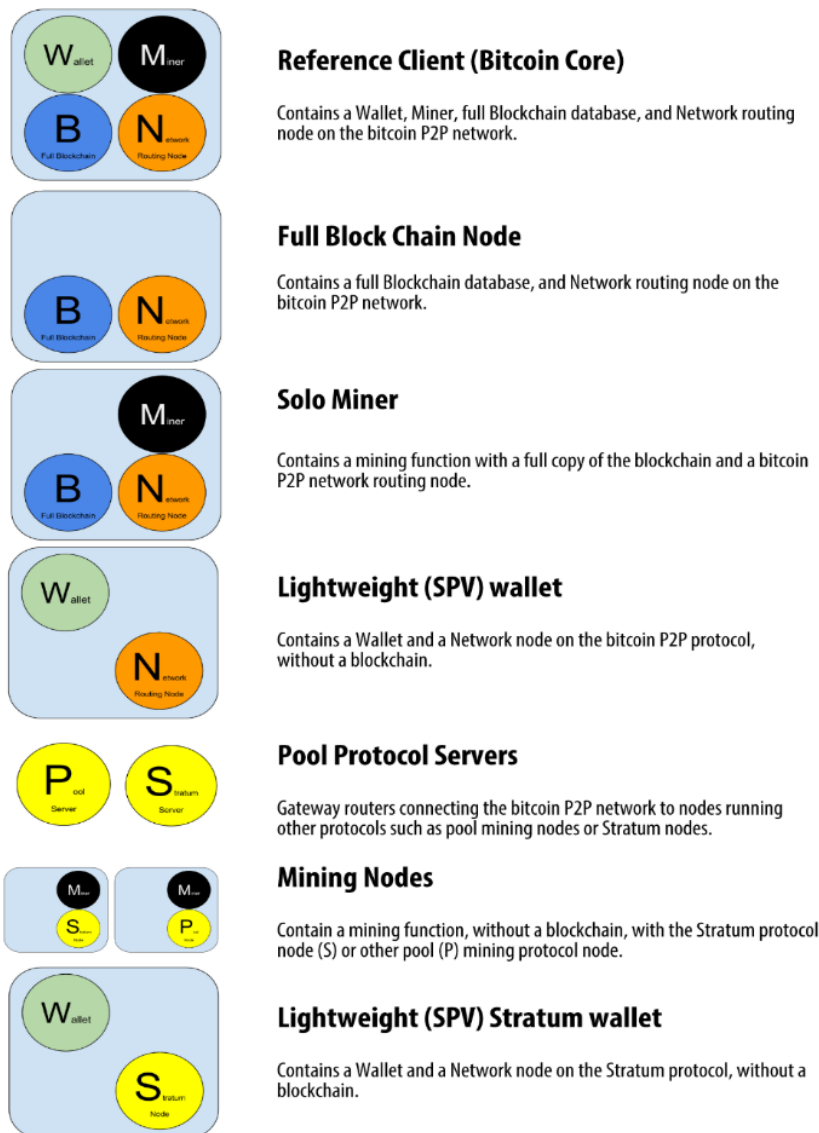
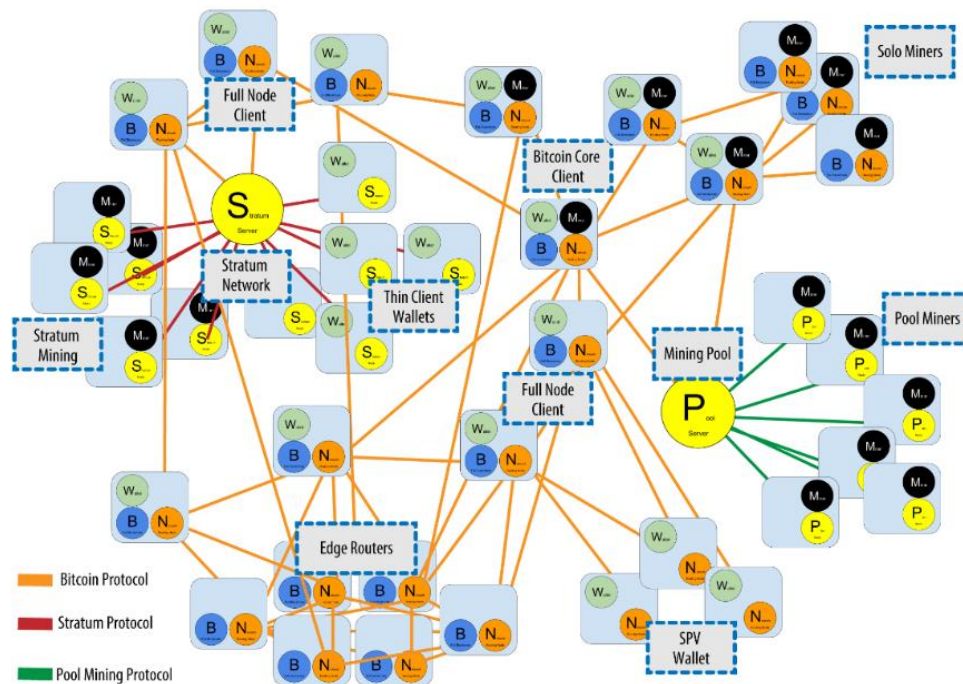


Figura 2: diagrama do sistema Bitcoin, com os vários tipos de nós.

Fonte: Antonopoulos (2014)



As transacções e a mineração:

A transacção (de bitcoins) é o elemento essencial deste sistema (Narayanan, 2017, p. 51; Antonopoulos, 2014, p. 109): foi com o objectivo de permitir transacções *online*, entre estranhos, que foi desenvolvido o Bitcoin, sendo a criação da unidade de conta digital, uma consequência desse objectivo. Aliás, pode dizer-se que todo o sistema foi architectado com o único objectivo de garantir a validade, a legitimidade, propagação e a segurança das transacções (Antonopoulos, 2014, p. 109).

Em virtude de ser uma rede descentralizada, e de não depender de instituições financeiras, Nakamoto introduziu o conceito de mineração (*mining*) para garantir a segurança do sistema e para validar as transacções – a analogia com a indústria mineira do ouro resulta da escassez inerente ao protocolo Bitcoin (máximo de 21 milhões de unidades) e do árduo trabalho para a sua “extracção” (a prova matemática denominada *proof-of-work*); daí que os agentes que verificam as transacções se denominem mineiros.

A mineração de Bitcoins cumpre duas funções: por um lado, verificar e certificar as transacções, por outro, permitir a emissão de novas unidades de Bitcoin. Para Beikverdi e Song (2015, n/d), a mineração desempenhada pelos mineiros é a função principal do sistema, o seu motor.

Os mineiros do Bitcoin agregam as transacções e produzem os blocos que são adicionados ao Blockchain. Para que um bloco seja válido todas as transacções nele contidas têm que ser válidas, com referência a blocos anteriores.

Adicionalmente, para que o bloco seja válido e adicionado ao Blockchain deve satisfazer a condição criptográfica *proof-of-work*, contendo o cabeçalho do bloco anterior (também este gerado de forma criptográfica). Esta função criptográfica é de difícil solução (funciona como tentativa e erro), mas fácil de verificar pelos demais mineiros.

Uma vez confirmada a validade do bloco pelos outros mineiros, através de consenso maioritário (os mineiros votam com a sua capacidade computacional; quanto mais poder computacional maior a capacidade de voto), o bloco pode ser adicionado ao Blockchain.

Os blocos são adicionados ao Blockchain a cada 10 minutos (em média). Por conterem todas as transacções já realizadas no sistema, desde o seu Bloco Génese (criado em 2009).

A tarefa dos mineiros é complexa e difícil de realizar. Por esse motivo, têm aparecido *softwares/hardwares* que permitem cumprir a função de mineração de forma mais eficaz (ASIC).

Porém estes *softwares/hardwares* são caros e de desgaste muito rápido, exigindo investimentos constantes e regulares. Além disso, o processo de mineração exige um gasto energético muito elevado, o que impede o acesso de muitos utilizadores ao negócio de mineração.

Estes factos têm levado muitos mineiros a associarem-se entre si, constituindo as designadas *pools* de mineiros, ou *mining pools*.

A existência destas associações de mineiros origina a concentração de poder (como veremos no próximo capítulo) no sistema, no que parece ser uma contradição com os objectivos de Nakamoto quando o criou.

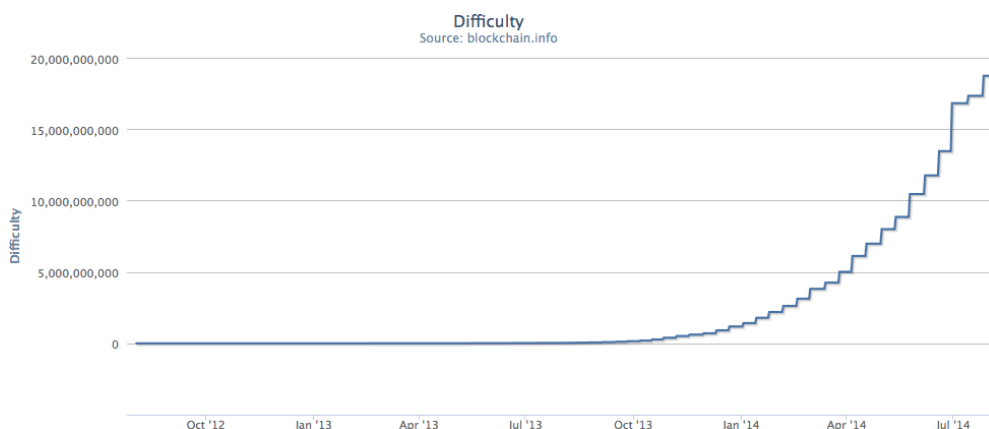
Gráfico 6: evolução do poder de computação.

Fonte: Antonopoulos (2014)



Gráfico 7: evolução da dificuldade do puzzle matemático.

Fonte: Antonopoulos (2014)



Versando agora o bitcoin (moeda), Ross (2016, p. 111) começa por indicar que se trata de uma moeda transnacional e que a sua aparição “oferece um caso de estudo para o futuro da moeda, à medida que se intensifica a codificação do dinheiro.” O mesmo autor caracteriza o bitcoin da seguinte forma:

“A *bitcoin* é uma «moeda digital» - uma moeda que é armazenada em código e transacionada *online*. É também uma «criptomoeda», um termo utilizado com frequência de forma intermutável com «moeda digital», mas que significa que a moeda utiliza métodos criptográficos numa tentativa de a tornar segura. (...) Num primeiro momento, a *bitcoin* parece caracterizar-se igualmente por uma dimensão de investimento. Tem as propriedades de um activo especulativo, sendo que o seu valor sobe e desce em enormes movimentos.” (Ross, 2016, p. 111-112).

Neste sentido, e tendo em conta as características do sistema, o Bitcoin é encarado como uma criptomoeda (*cryptocurrency*), como uma moeda digital, como uma moeda virtual, entre outras qualificações. Por outro lado, o Bitcoin também por ser visto como um bem (*asset*), ou como uma mercadoria (*commodity*).

A encriptação assimétrica (chaves públicas e privadas) é utilizada no sistema Bitcoin para manter o anonimato dos utilizadores. A chave pública é o endereço dos Bitcoins, e a chave privada funciona como *password* para validar transacções (Brito e Castillo, 2016, p. 7). Aliás, como refere Nakamoto (2014, p.), a titularidade dos Bitcoins é estabelecida através destas chaves.

Quando se contempla a faceta de moeda digital do Bitcoin, importa verificar a sua adequação ao próprio conceito de moeda, um conceito económico e social relativamente ao qual não existe

consenso, razão pela qual, a teoria económica recorre às funções que a moeda desempenha: meio de troca; unidade de conta; e, reserva de valor.

A este respeito, começamos por referir que o Bitcoin desempenha de forma eficiente a função de meio de troca. As transacções são rápidas e de baixo custo, o que permite reduzir de forma drástica os custos de transacção.

Por outro lado, e no que tange a função de unidade de conta, sublinhamos que o Bitcoin é divisível até à oitava casa decimal, o que permite enorme escala. No entanto, é uma moeda deflacionária o que pode ter consequências adversas.

Por fim, enquanto reserva de valor, a natureza deflacionária do Bitcoin impede a sua consideração como instrumento de reserva de valor. Além disso, esta natureza deflacionária pode originar pouca liquidez, no lado da oferta de moeda. Por outro lado, trata-se de uma moeda altamente volátil. Grande parte dos utilizadores prefere guardar os seus Bitcoin sem vez de os utilizar.

A volatilidade e natureza deflacionária:

Outra importante questão relativamente ao sistema Bitcoin relaciona-se com a grande volatilidade da sua unidade de conta: o bitcoin, ou BTC. Importa percebermos, então, que o valor desta unidade de conta não resulta de uma actuação intencional levada a efeito por uma entidade centralizada (como no sistema vigente, em que o valor de uma moeda é condicionado pelos diversos instrumentos monetários). Na verdade, o valor da unidade de conta BTC resulta apenas da procura (pela moeda) e da oferta (de moeda) no mercado.

Ora, a este respeito, importa sublinhar, desde já, dois aspectos essenciais: por outro lado, a procura depende, em grande medida, de eventos relativos ao próprio sistema e à sua aceitação pelos diversos Estados e pelos agentes económicos; por outro, a oferta não resulta de uma política monetária centralizada, antes resulta, apenas, da própria configuração do sistema, que prevê a criação de um limite máximo de bitcoins, de forma regular e constante (os bitcoins são gerados em resultado da criação de cada bloco, como vimos, sendo, simultaneamente, o incentivo económico para os operadores do sistema – os “mineiros”).

Gráfico 8: valorização no período 2017-01-02 / 2017-06-26

Fonte: <http://www.coindesk.com/price/>

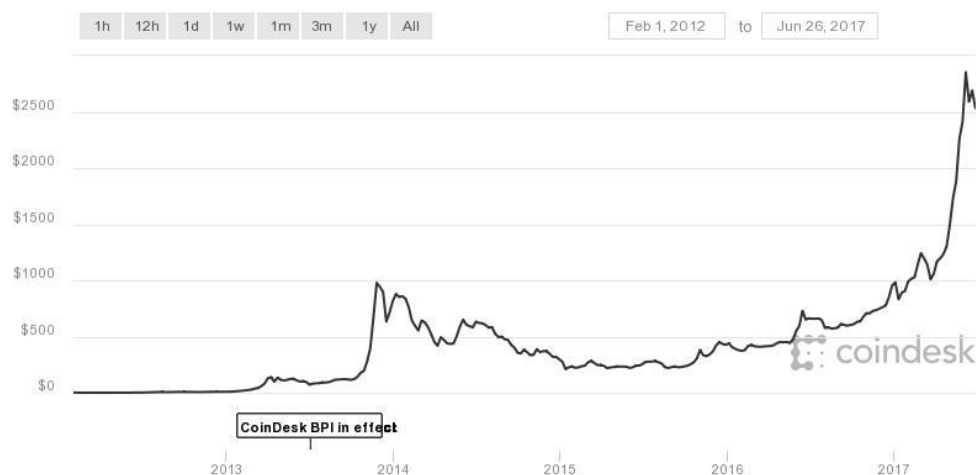
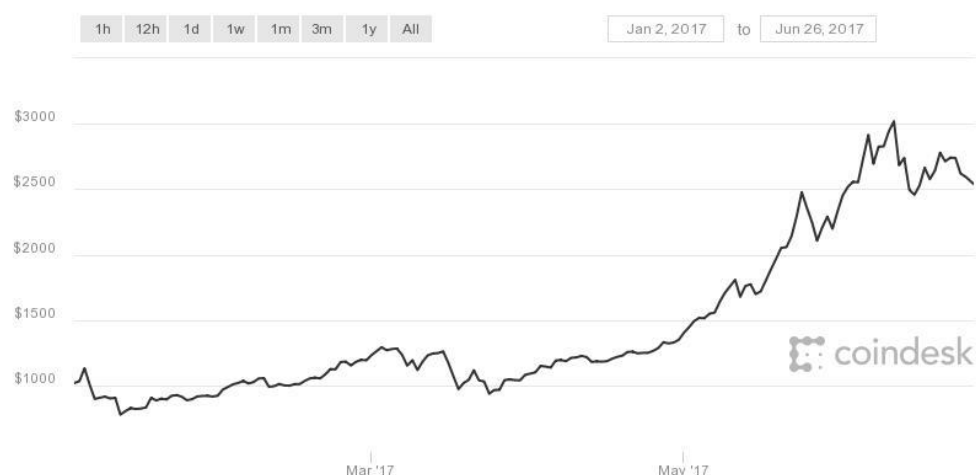


Gráfico 9: valorização no período 2017-01-02 / 2017-06-26.

Fonte: <http://www.coindesk.com/price/>



Ademais, o sistema Bitcoin, em si, ainda não foi violado, ou seja, podemos sustentar que a criptografia do *blockchain* é segura, e tem sido imune a ataques. No entanto, o facto de o registo das transacções (e a sua história) ainda não ter sido corrompido, não significa que o sistema não tenha fragilidades.

3.3. Aspectos positivos e negativos

A ideia de que a tecnologia Bitcoin é disruptiva é muito veiculada na sociedade, através tanto de especialistas como dos *media* generalistas³⁸.

3.3.1. Aspectos positivos

Anonimato:

O anonimato, ou melhor, a privacidade que o sistema de chaves públicas e privadas permite, pode ser visto como uma característica positiva pelos utilizadores que queiram fugir ao controlo das entidades reguladoras, mas também para quem valorize a sua privacidade.

Redução dos custos de transacção e aumento da velocidade:

Mougayar (2016, p. 38) O sistema Bitcoin permite uma redução de custos para os utilizadores. Os motivos que podem suscitar interesse na utilização do sistema Bitcoin tanto por empresas como por particulares são sensivelmente os mesmos: redução de custos de transacção; e, rapidez da transacção.

No entanto, e especificamente no que respeita às empresas, podemos acrescentar uma outra característica: o facto de as transacções serem definitivas. Com efeito, a (suposta) imutabilidade das transacções realizadas no sistema Bitcoin impede a ocorrência de *charge-backs* fraudulentos pelos consumidores – esta característica pode não agradar aos utilizadores/particulares.

Por seu turno, os particulares também podem ter interesse no sistema Bitcoin por uma outra característica: o anonimato das transacções. Na verdade, a realização de uma transacção pelos meios convencionais exige a partilha de inúmeros dados pessoais, o que deixa muitas pessoas preocupadas, num Mundo cada vez mais digital.

Estímulo à inovação financeira e tecnológica:

³⁸ O conceito de inovação disruptiva foi cunhado por Clayton M. Christensen, e refere-se a um avanço tecnológico que cria novo valor de mercado revolucionando o mercado existente. De acordo com Christensen (1997), a disrupção começa com soluções mais simples e mais baratas, na base de um mercado ou sector, e que gradualmente vão alargando a sua influência e adopção (movimento *upmarket*), destruindo indústrias estáveis.

Por outro lado, o sistema Bitcoin, e o Blockchain, é um forte catalisador de futura inovação tecnológica. Nomeadamente, enquanto plataforma descentralizada (distribuída), que permite registar e certificar transferências, alterações de propriedade, e *smart contracts*.

De facto, nos últimos tempos têm aparecido inúmeras inovações, seja no próprio ecossistema do Bitcoin, seja em outros âmbitos. Em grande medida, este potencial deve-se em grande medida, ao facto de o código do Bitcoin ser público (*open source*), o que significa que qualquer pessoa pode fazer o seu *download*, analisá-lo, melhorá-lo ou mesmo adaptá-lo para outros fins.

Potencial de redução da pobreza e opressão:

Por outro lado, o Bitcoin pode melhorar a condição de vida da significativa percentagem de população não banquerizada. Com efeito, em zonas remotas ou em zonas em vias de desenvolvimento, não é economicamente rentável para as instituições financeiras oferecer serviços financeiros. Esta população não banquerizada pode ascender a cerca 64% da população em países em vias de desenvolvimento (Brito e Castillo, 2016).

Enquanto sistema aberto e descentralizado, o Bitcoin pode providenciar o acesso a serviços financeiros a estas pessoas, de baixos rendimentos, tanto em países desenvolvidos como em vias de desenvolvimento.

O Bitcoin pode também ser uma forma barata e rápida para os emigrantes enviarem dinheiro para as suas famílias (*remittances*).

3.3.2. Aspectos negativos

Anonimato:

Costuma ser veiculado nos media que o Bitcoin é uma moeda anónima. No entanto, a designação correcta seria dizer que o Bitcoin é uma moeda pseudónima: as transacções não só são visíveis por todos (transparência), como ficam gravadas no Blockchain.

Todavia, em virtude de o Bitcoin integrar a encriptação de chaves assimétricas (chaves públicas e chaves privadas), a identidade dos autores e dos beneficiários das transacções não é divulgada. Como se referiu, esta característica do Bitcoin tanto pode ser um aspecto negativo como positivo (ver *supra*). Será negativo do ponto de vista das entidades reguladoras, pois fica difícil controlar a actividade de lavagem de dinheiro, de fuga ao fisco, e outras actividade criminosas.

Volatilidade da moeda:

Para o sistema Bitcoin funcionar da forma como foi arquitectado por Nakamoto, é essencial que as unidades de conta tenham grande circulação. Daí que a volatilidade seja vista como um aspecto negativo, já que, considerando a natureza deflacionária do bitcoin, os utilizadores tendem a guardar as suas moedas, em vez de as utilizarem.

Falhas de segurança:

Apesar de o sistema ainda não ter sido violado, já houve várias falhas no ecossistema Bitcoin³⁹. Na verdade, os pontos de informação centralizada, como por exemplo, os intermediários, representam o “calcanhar-de-aquiles” do sistema.

Utilização criminosa:

Quando consideramos que o sistema Bitcoin permite realizar transferências de dinheiro, online, de forma anónima, é legítimo presumir que tal anonimato pode potenciar a actuação criminosa de diversos agentes. Grande parte do criticismo relativamente ao Bitcoin versa, precisamente, o anonimato que permite a criminosos, nas suas operações ilícitas, seja de tráfico de droga, de armas, de seres humanos, lavagem de dinheiro, entre outras.

Paradigmático tem sido o exemplo do mercado *online Silk Road*, onde eram transacionados produtos ilícitos, na rede TOR, longe do olhar dos Estados e da sua capacidade de intervenção.

3.3.3. Desafios

Além destas características, devemos sublinhar alguns desafios que o Bitcoin enfrenta, quando encarado como uma mudança de paradigma (Tapscott, 2016).

Conhecimento tecnológico:

Um dos principais problemas reside no facto de a tecnologia em causa exigir vastos conhecimentos tecnológicos (pessoas muitas vezes não sentem segurança a trabalhar com algo que não dominam e tão complexo).

³⁹ O ecossistema do Bitcoin engloba todos os intervenientes do sistema, nomeadamente, os intermediários.

Acresce, ainda, que a adopção desta nova tecnologia carece de uma profunda mudança de comportamento dos utilizadores, que estão habituados a recorrer a intermediários para garantirem a segurança da informação, das transações, etc.

Associação a actividade criminosa:

Por outro lado, a primeira aplicação da tecnologia Blockchain, o Bitcoin, anda muitas vezes associada à actividade criminosa, o que pode impedir a sua adopção.

Necessidade de estrutura tecnológica:

Depois, o Blockchain exige uma complexa estrutura social e tecnológica. Enquanto inovação digital, e apesar de ser uma tecnologia transnacional e descentralizada, a adopção do sistema Bitcoin será diferente de país para país. No *THE GLOBAL INFORMATION TECHNOLOGY REPORT 2016* (WEF e INSEAD, 2016), apresenta-se um enquadramento da adopção de inovações tecnológicas, com base no índice NRI – *Networked Readiness Index*. Este índice avalia a preparação de cada país para a adopção de inovações tecnológicas, como base nos seguintes indicadores: 1. Ambiente tecnológico (político, regulatório, empresarial, inovação); 2. Preparação da rede (infraestrutura TIC, custos, capacidades e competências); 3. Adopção de tecnologia (empresas, governos, particulares); 4. Impacto económico e social.

Capacidade transaccional e liquidez:

Do ponto de vista do Bitcoin, ainda falta capacidade transaccional e liquidez (o mercado ainda é reduzido, e grande parte dos utilizadores guarda as suas unidades de conta), é pouco acessível e nada *user-friendly* para o consumidor médio.

Desemprego tecnológico de larga escala e poder de desintermediação:

Por outro lado, a inovação tecnológica associada ao Bitcoin e, em especial, ao Blockchain, têm potenciado o aparecimento de novas plataformas que procuram, cada vez mais, roubar espaço de actuação ao Estado, ou que pretendem substituir o modo como as estruturas governamentais são organizadas.

Por exemplo, têm aparecido várias iniciativas que pretendem utilizar a tecnologia Blockchain para serviços como: registos públicos (predial, comercial, civil); votação e eleições; outros.

A tecnologia subjacente ao Bitcoin, o Blockchain, pode provocar uma desintermediação transversal no sistema financeiro.

Falta de regulação do próprio sistema:

Ademais, a falta de enquadramento legal e de suporte dos Estados pode representar um enorme risco para os utilizadores de Bitcoin e, no limite, de outras manifestações da tecnologia Blockchain (todas têm um elemento de representação de valor monetário). Com efeito, e como vimos *supra*, o controlo das moedas e dos fluxos monetários é determinante para os Estados (Samuelson e Nordhaus, 2005; Friedman, 2014; Cohen, 1998).

3.4. A regulação do sistema Bitcoin

O sistema Bitcoin é uma tecnologia digital, que funciona numa plataforma global, descentralizada, beneficiando dos avanços tecnológicos (redes, *hardware* e *software*) que têm propulsionado a nova economia (digital). Um dos aspectos relevantes do *supra*-referido índice NRI é a regulação. Ora, como vimos antes, a globalização e a digitalização exigem novos paradigmas de actuação das entidades reguladoras. Esta realidade é particularmente importante no que respeita ao sistema Bitcoin, desde logo, pela sua natureza dual (moeda e sistema de pagamentos).

A regulação do Bitcoin deve ser encarada sob dois prismas: um, interno, que consiste na regulação do Bitcoin pelo próprio sistema – podemos falar aqui em governação; o outro, externo, que se materializa na possibilidade de regulação por entidades exteriores ao sistema – nomeadamente, os Estados e entidades reguladoras.

Relativamente à regulação interna, conforme se refere no *site* de referência Bitcoin.org, o protocolo Bitcoin não pode ser alterado sem a cooperação da maioria dos principais actores do sistema (os mineiros e os *developers*), que escolhem o *software* que utilizam, bem como as alterações que pretendem instituir. A regulação interna do sistema Bitcoin é, assim, um fenómeno de consenso maioritário.

Por outro lado, o sistema Bitcoin assenta numa rede descentralizada, não existindo um ponto de controlo individualizado, o que, como veremos, dificulta qualquer forma de regulação externa: não existe uma entidade responsável pelo sistema.

Em especial, no que respeita à regulação pelos Estados, acrescentamos o seguinte. Por um lado, o facto de ser uma moeda/sistema transnacional dificulta a regulação de forma isolada pelos Estados (limita a sua soberania e obriga à articulação de reguladores de vários países). Por outro lado, o facto de ser um sistema descentralizado dificulta a imputação de responsabilidades e até a aferição de riscos. Ademais, a falta de envolvimento de Bancos limita a protecção dos consumidores.

Por fim, o anonimato das transacções pode potenciar a utilização criminosa, dificilmente controlável pelas regras contra a Lavagem de Dinheiro (*Anti-Money Laundering* – AML) – Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão.

A título de exemplo, considere-se a dificuldade em identificar os utilizadores de Bitcoins (entidades autoras e beneficiárias dos pagamentos), em confronto com as regras KYC (*Know Your Customer*); ou o controlo de transacções superiores a certos limites ou com determinadas características; o sistema Bitcoin não está sujeito a tais restrições (no limite, podemos considerar que os intermediários possam estar ou vir a estar abrangidos por estas regulações).

4. INCONSISTÊNCIAS DO BITCOIN

4.1. A descentralização do sistema Bitcoin

A descentralização é, para Shin (2017, n/d), a mais importante característica do Bitcoin. Para Narayanan *et al* (2017, p. 27) o sistema Bitcoin consegue a descentralização através de uma combinação de métodos técnicos e de incentivos. Estes autores consideram que a resposta relativa à forma como o Bitcoin consegue a descentralização pressupõe a análise de cinco questões: 1. Quem mantém o livro-razão (*ledger*) das transacções (o Blockchain)? 2. Quem tem autoridade quanto à validade das transacções? 3. Quem cria novos Bitcoins? 4. Quem determina as alterações às regras do sistema? 5. Como é que os Bitcoins adquirem valor de troca? Estes autores defendem que a rede *peer-to-peer*, do sistema Bitcoin, é quase descentralizada, por considerarem que qualquer pessoa pode ser um nó no sistema, sendo as barreiras à entrada praticamente inexistentes (como se trata de um artefacto digital, a sua reprodução tem um custo próximo de zero). Reconhecem, por outro lado, que a mineração de Bitcoins também é aberta a qualquer um, de um ponto de vista técnico. Porém, o facto de ser uma actividade de capital intensivo resulta na existência de barreiras à entrada, e que tal facto leva à centralização e à concentração de poder.

Para Narayanan *et al* (2017, p. 28-32), o sistema funciona com base em consenso distribuído (que exige a demonstração do esforço empreendido – *proof-of-work*), entre os nós do sistema, que têm que concordar relativamente à verdade histórica das transacções. Sendo a rede *peer-to-peer* do sistema Bitcoin imperfeita, Nakamoto introduziu os conceitos de incentivos e de aleatoriedade (*randomness*), o que, segundo estes autores, permite um bom funcionamento do Bitcoin.

Para Beikverdi e Song (2015, n/d), os sistemas de pagamentos distribuídos (descentralizados) enfrentam vários problemas, que se podem agrupar em três categorias: correcção (garantir a inexistência de transacções fraudulentas), concordância (entre os nós do sistema quanto a uma única verdade – o Blockchain é igual para todos) e utilidade (do sistema, que inclui a acessibilidade e a facilidade de utilização).

Em virtude de não existir uma autoridade central a garantir a segurança e a validade do sistema, Nakamoto introduziu o conceito de mineração (*mining*), que, como vimos, desempenha duas funções no sistema (Beikverdi e Song (2015, n/d): por um lado sincronizar e validar as transacções; por outro, permitir a emissão de novas moedas.

4.1.1. A tendência de centralização

Para Narayanan *et al* (2017, p. 27-26) a noção de competição entre paradigmas de centralização e de descentralização é comum em diversas tecnologias digitais, e reconhecem que a descentralização não deve ser encarada como um “tudo ou nada”: quase nenhum sistema é absolutamente descentralizado ou absolutamente centralizado.

Segundo Beikverdi e Song (2015, n/d), o sistema Bitcoin assistiu, desde 2013, a um processo de centralização, em virtude da existência de carteiras digitais (intermediários) e de mineração centralizada. Courtois e Bahack (2014, n/d) defendem, a este respeito, que “o Bitcoin não é (ou ainda não é) esta espécie de utopia de rede descentralizada que não pertence a ninguém e funciona para toda a gente, como às vezes se diz ser. É preciso parar de se dizer que o Bitcoin é uma utopia que nunca foi, e encará-lo como um jogo com múltiplos participantes, cada um com os seus interesses particulares.” Também neste sentido, Gervais *et al* (2014, p. 1) sublinham que, em virtude de os mineiros “votarem” com o seu poder computacional, existia a crença de que nenhum mineiro conseguiria dominar uma significativa capacidade de voto. Estes autores defendem que, apesar de a mineração e a geração de blocos terem sido desenhadas para serem descentralizadas, estes processos são, hoje em dia, largamente centralizados.

Faggart (2015, n/d) salienta que, para percebermos o fenómeno da centralização, importa identificarmos as forças económicas que a podem causar, que resume no conceito de “economias de escala”.

Carteiras digitais:

Como vimos *supra*, a utilidade (que inclui a acessibilidade e a facilidade de utilização), é uma característica essencial dos sistemas distribuídos. Ora, o protocolo Bitcoin é complexo, e a utilização do sistema Bitcoin não é uma tarefa fácil. Além disso, Gervais *et al* (2014, p. 4) salientam que, para um utilizador particular, a instalação do sistema requer também muito espaço de disco rígido.

Por estes motivos, começaram a aparecer intermediários, como as carteiras virtuais, casas de câmbio, entre outros, para facilitar a utilização e o acesso, aos utilizadores sem os conhecimentos técnicos do sistema (Beikverdi e Song, 2015, n/d; Gervais *et al*, 2014, p. 4)

Sucedem que, estes intermediários funcionam sob lógicas de centralização, semelhantes às do sistema bancário. Ao centralizarem informação, tronam-se pontos frágeis do sistema, podendo

ser vítimas de ataques informáticos, com consequências desastrosas para os seus clientes (a este respeito, considere-se o caso da falência da empresa MtGox) (Beikverdi e Song (2015, n/d).

Mineração centralizada:

Por outro lado, e como vimos *supra* também, a dificuldade dos puzzles matemáticos que os mineiros têm de resolver tem vindo a aumentar. Em virtude desta dificuldade, e da minúscula probabilidade de um mineiro isolado conseguir o prémio pela resolução do puzzle (atribuição de novos Bitcoins, além das comissões relativas às transacções incluídas no bloco) os indivíduos que pretendem participar no sistema Bitcoin tendem a agrupar-se com outros mineiros (Beikverdi e Song, 2015, n/d; Gervais *et al*, 2014, p. 3).

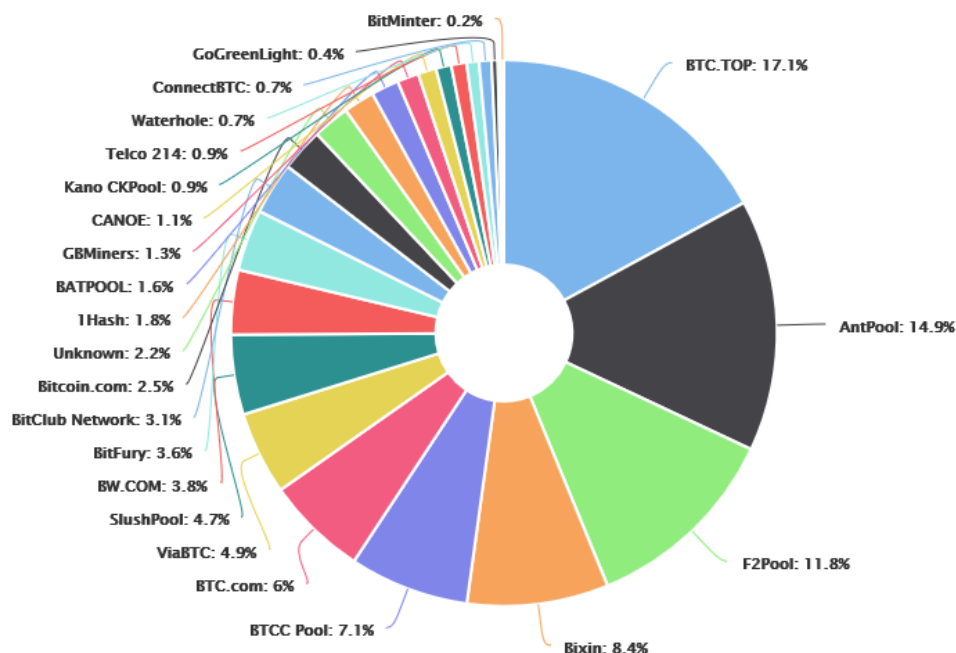
Por este motivo, desenvolveu-se o conceito dos grupos de mineiros (*mining pools*). Nestes grupos, os mineiros combinam as várias capacidades computacionais, aumentando a probabilidade de resolução do puzzle matemático e consequente partilha do prémio. Para Courtois e Bahack (2014, n/d), estes agrupamentos permitem reduzir a incerteza dos retornos (da lotaria) e garantir um rendimento regular (Gervais *et al*, 2014, p. 3).

Por outro lado, e em virtude da apreciação do Bitcoin, o processo de mineração vai-se tornando cada vez mais competitivo (entrada de novos players). Este facto tem levado a uma grande evolução, também, do *hardware* e do *software* utilizado na mineração. Se no início era possível minerar Bitcoins (e com isso garantir a segurança do sistema) com um simples computador pessoal, actualmente, o processo de mineração só consegue ser realizado com eficácia mediante o recurso a *hardware/software* ASIC.

Como referem Beikverdi e Song (2015, n/d), a ineficiência e a falta de incentivos adequados, combinadas com a reduzida probabilidade de solução dos puzzles por indivíduos, tem levado a um decréscimo de nós no sistema, que preferem partilhar a sua força computacional num agrupamento de mineiros, tornando a rede Bitcoin cada vez mais centralizada.

Segundo Gervais *et al* (2014, p. 3), se os agrupamentos de mineiros conseguirem mais do que 50% da capacidade computacional da rede, conseguirão controlar, de forma efectiva, a confirmação de todas as transacções registadas no sistema (incluindo-se aqui, a não realização de determinadas transacções, a aprovação de determinadas transacções e transacções de gasto duplo). No Gráfico 10 podemos ver a concentração existente na mineração de Bitcoins.

Gráfico 10: Distribuição da taxa de *hash* (capacidade computacional), entre agrupamentos de mineiros (*mining pools*)



Actualizações do protocolo Bitcoin:

Segundo Gervais *et al* (2014, p. 4), só os *developers* têm autoridade para realizar as necessárias modificações e actualizações ao protocolo Bitcoin (estes *developers* são, como vimos, uma espécie de administradores do protocolo). Sucede que, os developers do sistema Bitcoin não são mais do que duas dezenas de pessoas, o que leva estes autores a defender que o sistema, relativamente a este aspecto, é altamente concentrado - Shin (2017, n/d) qualifica esta situação como *developer centralization*.

Acresce que, nem os utilizadores do Bitcoins nem os mineiros têm algum poder de escolha quanto à nomeação dos *developers* (Gervais *et al*, 2014, p. 2).

Os *developers* são, ainda, os responsáveis pela decisão sobre qual o Blockchain mais longo quando existe uma bifurcação no sistema (*fork*), sendo certo que, o Blockchain não escolhido deixa de existir, tal como as transacções aí realizadas e inscritas por uma parte da rede (Gervais *et al*, 2014, p. 5). Ademais, também cabe aos *developers* a emissão de alertas, nomeadamente, os alertas referentes a endereços suspeitos (moedas suspeitas – *tainted coins*), que perderão o seu valor, em função de não serem aceites pela rede Bitcoin em futuras transacções (Gervais *et al*, 2014, p. 6).

Não obstante, as decisões referentes às alterações do protocolo (as mais importantes) só são adoptadas pelo sistema se a maioria da capacidade computacional, ou seja, se a maioria dos mineiros, assim o entender.

Certo é que, como referem Gervais *et al* (2014, p. 6), o facto de o poder estar concentrado pode facilitar a pressão dos Estados e das entidades reguladoras.

Centralização do mercado de transacções:

Shin (2017, n/d) refere também a existência de um mercado de transacções centralizado. Para esta autora, o sistema Bitcoin não tem conseguido resolver o problema do aumento do volume de transacções perante uma rede cuja capacidade estagnou, levando a um aumento de comissões cobradas por transacção. Este facto, segundo Garzik (*apud* Shin, 2017, n/d) “empurra” os utilizadores para intermediários virtuais (centralizados).

Por outro lado, Shin (2017, n/d) põe ainda em evidência o facto de a incapacidade da rede perante o avolumar de transacções se reflete, também, a demoras no registo de muitas transacções.

Em sentido concordante, Baxter (2017, n/d) faz uma analogia entre os mineiros e as portagens da autoestrada, sustentando que ambos funcionam da mesma forma: os mineiros adoram que exista muito tráfego pois isso representa mais comissões (*transaction fees*). No entanto, sublinha o mesmo autor que as comissões pagas no sistema Bitcoin têm vindo a aumentar, tal como o tempo de espera na confirmação das transacções (*transaction confirmation times*), apesar de o número de transacções só ter aumentado de forma modesta.

Gráfico 11: crescimento das comissões de transacção.

Fonte: Baxter (2017)



Gráfico 12: crescimento volume de transacções.

Fonte: Baxter (2017)



Teoria das redes:

Beikverdi e Song (2015, n/d) salientam que a centralização é um fenómeno que se verifica naturalmente em muitos sistemas, por permitir uma maior simplificação dos mesmos. No entanto, no caso do Bitcoin a centralização é uma ameaça, que pode pôr em causa a segurança do próprio sistema, na medida em que a descentralização é um pressuposto da segurança.

4.1.2. Impactos da centralização

Segurança do sistema:

Nakamoto (2008, p. 1) referiu que o sistema Bitcoin é seguro desde que metade dos mineiros (os nós do sistema) seja honesta. No entanto, a existência de agrupamentos de mineiros faz perigar a segurança do sistema, tornando possíveis diversos tipos de ataques. Por exemplo, um agrupamento de mineiros, que tenha mais de 51% por cento do poder computacional, da rede Bitcoin, pode desencadear um designado *51% Attack*, mediante o qual consegue subverter as regras do sistema, manipulando as transações (Beikverdi e Song, 2015, n/d). Shin (2017, n/d) refere que os ataques de rede podem ser de três tipos: violação da confidencialidade, da disponibilidade ou da integridade.

Courtois e Bahack (2014, n/d) descrevem vários tipos de ataques, além do *51% Attack*, que se traduzem em possíveis estratégias subversivas dos mineiros, alguns dos quais não carecem, sequer, de largas maiorias (de poder computacional) para provocar danos ao sistema: *Pool Hopping Attack*; *Mining Cartel Attack*; *Difficulty Raising Attack*; *Confidential Cryptographic Optimization Attack*; *Selfish Mining Attack*; *Block Discarding Attack*; *Block Withholding Attack*.

Em função destes factos, a mineração centralizada é considerada uma séria ameaça ao sistema (Beikverdi e Song, 2015, n/d; Shin, 2017, n/d). Para Courtois e Bahack (2014, n/d), “O Bitcoin cultiva o sonho “impossível” dos criptógrafos, de criar um sistema de pagamentos sem intermediários de confiança. Na teoria, o Bitcoin é uma rede que, supostamente, se policia a si própria. (...) Na prática, contudo, (...) nem todos os comportamentos subversivos são detectáveis. Se um determinado comportamento não desejado não for visível, dificilmente será policiado ou prevenido.”

A confiança e o Bitcoin:

Para Nakamoto (2008, p. 1), um dos principais problemas do sistema vigente residia na existência de “intermediários de confiança”, e pretendeu substituir estes intermediários por um protocolo matemático e informático – o “Protocolo da Confiança” de Tapscott (2016, p. 6).

Dodd (2017, p. 4) questiona esta análise, sustentando que, a crença de que o sistema Bitcoin substitui os intermediários de confiança por um protocolo de confiança é uma fantasia. Shin (2017, n/d) refere que, esta tecnologia, que prometia substituir a confiança nas instituições financeiras, bem como nos governos, mediante a implementação de um código matemático e informático, está tão susceptível às dinâmicas políticas e de poder como qualquer outro sistema.

A centralização do sistema, além de poder pôr em perigo a sua integridade, pode também abrir a porta à existência de gasto duplo (*double spend*), mediante o *51% Attack*, o que pode ser ruinoso para a reputação do Bitcoin (Faggart, 2015, n/d).

4.2. A função de pagamentos (meio de troca)

Como vimos *supra* no Capítulo II, a moeda desempenha três funções: meio de troca, unidade de conta e instrumento de reserva de valor. De acordo com Guadamuz e Marsden (2014, p. 4), as moedas foram inventadas, principalmente, com o objectivo de facilitar a troca, para facilitar, no fundo, as transacções entre as partes.

No Capítulo III vimos que o Bitcoin desempenha eficazmente as funções de meio de troca e de unidade de conta. Porém, o Bitcoin já não funciona como reserva de valor, em virtude da sua volatilidade, perante outras moedas.

Estas características resultam, segundo Guadamuz e Marsden (2014, p. 6), da própria arquitectura do protocolo Bitcoin, que integra a escassez como uma, limitando a oferta monetária, no que se pode caracterizar como natureza deflacionária do Bitcoin.

Para Antonopoulos (2014, p. 176), o facto de a oferta monetária ser fixa e predeterminada faz com que o Bitcoin tenha uma natureza deflacionária. Neste sentido, a deflacção do Bitcoin corresponde à falta de correspondência entre a procura e a oferta de moeda, no mercado.

De acordo com o mesmo autor, na prática, esta natureza tem originado um instinto de não utilização dos Bitcoins (*Bitcoin hoarding*). No entanto, Antonopoulos (2014, p. 176) considera que este instinto pode ser ultrapassado se o mercado estiver em condições de oferecer descontos ao consumidor.

Em sentido contrário, Guadamuz e Marsden (2014, p. 7) sublinham que,

“O verdadeiro número de BTCs em circulação é muito inferior ao previamente pensado, com 78% da reserva inteira de BTC (7.019.100 BTC) colocadas em endereços que estão guardados, e apenas 22% de todos os BTCs criados (incluindo os perdidos) em circulação. Isto confirma a suspeita de que o sistema encoraja a acumulação e não utilização, o que faz com que o Bitcoin não seja apto a desempenhar a função de moeda. Um grande número de transacções parecem consistir em operações entre o mesmo utilizador, sendo as moedas transferidas de um endereço para outro.”

Hanley (2015, p. 9) parece concordar com esta segunda posição, sustentando que nenhum agente racional utilizaria os Bitcoins, em valorização, para propósitos de consumo, acrescentando que, com esta arquitectura, o valor dos Bitcoins será sempre determinado pela especulação financeira e nunca pela utilidade que possa ter enquanto meio de pagamento.

5. CONCLUSÕES

O advento da tecnologia Bitcoin representa um marco na evolução da própria internet, já de si revolucionária, em múltiplos sentidos. Esta tecnologia permite transferir valor (entre outros bens digitalizados) num novo modelo, modelo este que nos faz questionar o papel e a presença de muitos intermediários. No fundo, esta tecnologia permite uma forte desintermediação na sociedade.

No entanto, o Bitcoin é uma tecnologia diferente, no sentido em que afecta a capacidade de os Estados planearem e executarem as políticas económicas, porquanto dificulta o controlo sobre os movimentos de capitais. Considerando este aspecto, é natural que o Bitcoin enfrente resistência dos Estados.

Por outro lado, também não podemos esquecer que o Bitcoin pode ser visto como alternativa aos bancos e outras instituições financeiras. Desde logo, pela eficiência e pela redução dos custos associados às transacções. No entanto, e relativamente a este plano, cabe sublinhar que o sistema Bitcoin, ao contrário do que é usualmente anunciado, é centralizado em muitos níveis (mineiros, *developers*, *wallets*), facto que pode causar falta de credibilidade do sistema e descrença dos utilizadores.

Ademais, a natureza deflacionária dificulta a sua consideração como moeda, e potencia a utilização do sistema Bitcoin pelos especuladores, com vista a ganhos futuros.

A presente investigação permitiu-nos, também, definir algumas avenidas de investigação futura. Em primeiro lugar, cremos ser importante analisar o nível de conhecimento e vontade de adesão ao Bitcoin (e particularmente, a sistemas montados no sistema Blockchain) pela população portuguesa. Depois, as oportunidades que o Blockchain encerra merecem também um estudo autónomo, comparando várias plataformas e modelos distintos, desenvolvidos com este protocolo (e respectivas alterações). Em terceiro lugar, seria interessante estudar a estrutura de incentivos, os tipos de rede e as dinâmicas de poder nos principais sistemas baseados em Blockchain. Por fim, com particular interesse, o estudo das plataformas que permitem a realização e execução de *smart contracts*, o seu funcionamento e a forma como podem ser disruptivas no sector do Direito.

BIBLIOGRAFIA

- Adriano, Andreas e Monroe, Hunter (2016), The internet of trust, *Finance & Development*, Junho, Vol. 53, n.º 2, p. 44-47.
- Alt, Rainer e Puschmann, Thomas (2012), The rise of customer-oriented banking - Electronic markets are paving the way for change in the financial industry, *Electron Markets* (2012) 22:203–215, DOI 10.1007/s12525-012-0106-2.
- Antonopoulos, Andreas (2015), *Mastering bitcoin*, Sebastopol (USA): O'Reilly.
- Arvidsson, Niklas (2014), A study of turbulence in the Swedish payment system – is there a way forward?, *foresight*, VOL. 16 n.º. 5, 2014, pp. 462-482, DOI 10.1108/FS-06-2013-0024.
- Ayres, Robert e Williams, Eric (2004), The digital economy: Where do we stand?, *Technological Forecasting & Social Change*, 71, 315 – 339.
- Bento, Vítor (2004), *Os estados nacionais e a economia global*, Coimbra: Livraria Almedina.
- Bheemaiah, Kariappa (2017), *The blockchain alternative: Rethinking macroeconomic policy and economic theory*, Berkley (USA): aPress.
- Brito, Jerry e Castillo, Andrea (2016), *Bitcoin: A primer for policymakers*, Washington (USA): Mercatus Center at George Mason University.
- Brito, Jerry; Hoegner, Stuart; Anning, Paul; Brazell, Lorna; Brailsford, Mark; Cleary, Matthew; Friedman, Jillian; Taylor, Michael; Strauss, Ryan; e, Von Unruh, Christoph-Nikolaus (2015), *The law of bitcoin*, Bloomington (USA): iUniverse.
- Brynjolfsson, Erik e Saunders, Adam (2010), *Wired for innovation: How information technology is reshaping the economy*, Massachusetts (USA): Massachusetts Institute of Technology Press.

- Carboni, Davide (2017), *Bitcoin under the mattress*, Reino Unido: digitaldavide.me
- Carvalho, Rui Moreira de (2011), *Compreender + África – Fundamentos para competir no mundo*, 2.^a Edição, Lisboa: Temas & Debates, Círculo de Leitores.
- Carvalho, Rui Moreira de (2014), *A força das coisas*, Lisboa: bnomics.
- Castells, Manuel (2002), *The rise of the network society*, 2.^a Edição (reimpressão), Massachusetts (USA): Blackwell Publishers.
- Cohen, Benjamin (1998), *The geography of money*, New York (USA): Cornell University Press.
- Cohen, Benjamin (2015), *Currency power: Understanding monetary rivalry*, New Jersey (USA): Princeton University Press.
- Cunha, António (1986), *Dicionário etimológico: Nova fronteira da língua portuguesa*, 2.^a Edição, Rio de Janeiro (Brasil): Editora Nova Fronteira.
- Daniel, Jean-Marc (2013), *8 Lições de história económica – Crescimento, crise financeira, reforma fiscal, despesa pública*, Coimbra: Actual.
- De Filippi, Primavera e Loveluck, Benjamin (2016). The invisible politics of bitcoin: Governance crisis of a decentralised infrastructure. *Internet Policy Review*, Volume 5, Número 3. DOI: 10.14763/2016.3.427
- Dias, Patrícia (2014), *Viver na sociedade digital – Tecnologias digitais, novas práticas e mudanças sociais*, Cascais: Princípia.
- Diniz, Francisco (2010), *Crescimento e desenvolvimento económico – Modelos e agentes do processo*, 2.^a Edição, Lisboa: Edições Sílabo.
- Dodd, Nigel, (2017), *The social life of bitcoin*. Theory, Culture & Society. ISSN 0263-2764

- Drucker, Peter (2007), *Sociedade pós capitalista*, 3.^a Edição, Lisboa: Actual Editora.
- Eco, Umberto (1984), *Como se faz uma tese em ciências humanas*, 3.^a Edição, Lisboa: Editorial Presença.
- Fernandes, Abel e Mota, Paulo (2015), *A teoria e a política monetárias na actualidade*, 3.^a Edição, Coimbra: Almedina.
- Finuras, Paulo (2013), *O dilema da confiança: Teorias, estudos e interpretações*, 1.^a Edição, Lisboa: Edições Sílabo.
- Fisher, Irving (2015), *A ilusão monetária*, Coimbra: Conjuntura Actual Editora.
- Floridi, Luciano (2014, 2016) *The 4th revolution: How the infosphere is reshaping human reality*, Oxford (UK): Oxford University Press.
- Friedman, Milton (2014), *Capitalismo e liberdade*, Coimbra: Actual Editora.
- Ferrari, Rossella (2015), Writing narrative style literature reviews, *Medical Writing* 2015, Volume 24, Número 4, p. 230-235.
- Gamble, Andrew (2009), *The spectre at the feast – Capitalist crisis and the politics of recession*, Hampshire (UK): Palgrave Macmillan.
- Gervais, Arthur; Karame, Ghassan; Capkun, Vedran; e Capkun, Srdjan (2014), Is bitcoin a decentralized currency? *IEEE Security & Privacy*. Volume 12, Número 3, Maio-Junho 2014.
- Green, Bart, Johnson, Claire e Adams, Alan (2006), Writing Narrative Literature Reviews for Peer-Reviewed Journals: Secrets of the Trade, *Journal of Chiropractic Medicine*, February 2006, p. 101-117.
- Han, Byung-Chul (2106), *No enxame: Reflexões sobre o digital*, Lisboa: Relógio D'Água Editores.

- Harari, Yuval (2017), *Homo Deus: A brief history of tomorrow*, London (UK): Vintage.
- Hayek, Friedrich (1990), *Denationalisation of Money – The Argument Refined: An Analysis of the Theory and Practice of Concurrent Currencies*, 3.^a Edição, London (UK): The Institute of Economic Affairs.
- Ingham, Geoffrey (2004), *The nature of money*, Cambridge (UK): Polity Press.
- Ingham, Geoffrey (2016), *Capitalism*, Reimpressão, Cambridge (UK): Polity Press.
- Innerarity, Daniel (2009), *A sociedade invisível: Como observar e interpretar as transformações do mundo actual*, Lisboa: Editorial Teorema.
- Innerarity, Daniel (2011), *O futuro e os seus inimigos: Uma defesa da esperança política*, Lisboa: Teorema.
- Jayaraman, Karthik (2012), Tragedy of the commons in the production of digital artifacts, *International Journal of Innovation, Management and Technology*, Vol. 3, No. 5, October 2012, DOI: 10.7763/IJIMT.2012.V3.308.
- Kondratieff, Nicolas (1982), The long waves in economic life, in *Cycles – Foundation Reprint*, Julho 1982, p. 151-154.
- Kondratieff, Nicolas (1982), The long waves in economic life, in *Cycles – Foundation Reprint*, Maio/Junho 1982, p. 107-111.
- Kotler, Philip, Kartajaya, Hermawan, e Setiawan, Iwan (2017), *Marketing 4.0: Mudança do tradicional para o digital*, Lisboa: Actual Editora.
- Kroll, Joshua, Davey, Ian e Felten, Edward (2013), The economics of bitcoin mining, or bitcoin in the presence of adversaries, *The Twelfth Workshop on the Economics of Information Security (WEIS 2013)*, Washington, DC, June 11-12, 2013.
- Kuhn, Thomas (2009) *A estrutura das revoluções científicas*, Lisboa: Guerra e Paz Editores.

- Langley, Paul e Leyshon, Andrew (2016), Platform capitalism, The intermediation and capitalisation of digital economic circulation, *Finance and Society*, *EarlyView* 1-21.
- Martin, Felix (2013), *Dinheiro: A biografia não autorizada*, 1.^a Edição, Lisboa: Temas & Debates – Círculo de Leitores.
- Maslow, Abraham (1954, 1970), *Motivation and personality*, New York (USA): Harper & Row, Publishers.
- McMillan, Jonathan (2014), *The end of banking: Money, credit, and the digital revolution*, Zurich: Zero/One Economics.
- Meiklejohn, Sarah, Pomarole, Marjori, Jordan, Grant, Levchenko, Kiril, McCoy, Damon, Voelker, Geoffrey, Savage, Stefan (2013) A fistful of bitcoins: Characterizing payments among men with no names. *Proceedings of the ACM SIGCOMM Internet Measurement Conference, IMC* (pp. 127-139). DOI: 10.1145/2504730.2504747.
- Mendes, Adriana (2013), *Transição de Basileia II para o Basileia III: “Qual o enfoque que é dado aos Riscos nos Acordos de Basileia?”*, Dissertação de Mestrado, Instituto Superior de Economia e Gestão.
- Middelkoop, Willem (2017) *O grande reajustamento – As guerras do ouro e o xaque-mate financeiro*, Coimbra: Actual Editora.
- Mougayar, William (2016), *The business blockchain – Promise, practice, and application of the next internet technology*, New Jersey (USA): Wiley.
- Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew, Goldfeder, Steven (2016) *Bitcoin and cryptocurrency technologies: A comprehensive introduction*, New Jersey (USA): Princeton University Press.
- Nunes, Ana Bela, e Valério, Nuno (2012), *O crescimento económico moderno – Introdução a uma história da economia mundial contemporânea*, 3.^a Edição, Lisboa: Editorial Presença.

- Parker, Geoffrey, Van Alstyne, Marshall, e Choudary, Sangeet (2016), *Platform revolution: How networked markets are transforming the economy--and how to make them work for you*, New York (USA): W. W. Norton & Company.
- Plassaras, Nicholas (2013), Regulating digital currencies: Bringing bitcoin within the reach of the IMF, *Chicago Journal of International Law*, Summer 2013, Vol. 14, N.º 1.
- Quivy, Raymond, e Campenhoudt, L. V. (2013), *Manual de investigação em ciências sociais*, 6.ª Edição, Lisboa: Gradiva.
- Roberts, Carl (2010). *The dissertation journey*. Thousand Oaks, CA: Corwin.
- Ross, Alec (2016), *As indústrias do futuro*, Coimbra: Actual Editora.
- Roth, Felix (2009), *The effects of the financial crisis on systemic trust*, Centre for European Policy Studies Working Document n.º 316. Disponível em:
<https://ssrn.com/abstract=1438510> ou <http://dx.doi.org/10.2139/ssrn.1438510>
- Rothstein, Adam and New Scientist (2017), *The end of Money – The story of bitcoin, cryptocurrencies and the blockchain revolution*, London: John Murray Learning.
- Samtani, Sanya e Baliga, Varun (2015) On Monopolistic Practices in Bitcoin: A Coded Solution, *The Indian Journal Of Law And Technology*, Volume 11, p. 106-116.
- Samuelson, Paul A., e Nordhaus, William D. (2005) *Economia*, 18.ª Edição, Lisboa: McGraw-Hill.
- Santos, Mário Coutinho dos (2015), *O dinheiro*, Lisboa: Fundação Francisco Manuel dos Santos.
- Schwab, Klaus (2017), *The fourth industrial revolution*, Londres (UK): Portfolio Penguin.
- Schultz, Ron (2013), Adjacent opportunities: The collaboration economy. *E:CO Issue*, Volume 15, N.º 4, p. 144-146.

- Shi, Ning (2016), A new proof-of-work mechanism for bitcoin, *Financial Innovation*, Dezembro 2016, p. 2:31. DOI: 10.1186/s40854-016-0045-6
- Silva, Eduardo (2012), *Dicionário de finanças e negócios internacionais*, Porto: Vida Económica.
- Silva, Eduardo, Mota, Carlos, Queirós, Mário e Pereira, Adalmiro (2013), *Finanças e gestão de riscos internacionais*, Porto: Vida Económica.
- Tapscott, Don (2014), *The Digital Economy – Anniversary Edition: Rethinking Promise and Peril in the Age of Networked Intelligence*, 2.^a Edição, New York (USA): McGraw Hill.
- Tapscott, Don e Tapscott, Alex (2016), *Blockchain revolution: How the technology behind bitcoin is changing money, business and the world*, USA: Portfolio Penguin.
- Tasca, Paolo, (2016), The dual nature of bitcoin as payment network and money, *VI Chapter SUERF Conference Proceedings 2016/1 "Cash on Trial"*, por Christian Beer, Ernest Gnan and Urs W. Birchler. <https://ssrn.com/abstract=2805003> e <http://dx.doi.org/10.2139/ssrn.2805003>
- Toffler, Alvin (1980), *The third wave*, New York: William Morrow and Company.
- Tonkiss, Fran (2009), Trust, confidence and economic crisis, *Intereconomics*, Julho/Agosto 2009, Volume 44, Número 4, p. 196–202.
- Tsyganov, Serhiy e Apalkova, Viktoriya (2016), Digital economy: A new paradigm of global information society, *Ekonomické Rozhl'ady – Economic Review*, Volume 45, N.º 3, p. 295-311.
- Ulrich, Fernando (2014), *Bitcoin – A moeda na era digital*”, São Paulo (Brasil): Instituto Ludwig Von Mises Brasil.
- Valdez, Stephen e Molyneux, Philip (2010), *An introduction to global financial markets*, 6.^a Edição, Hampshire (UK): Palgrave Macmillan.

- Vigna, Paul, e Casey, Michael J. (2016), *Cryptocurrency – The future of money?*, London: Vintage.
- Wälti, Sébastien (2012), Trust no more? The impact of the crisis on citizens' trust in central banks, *Journal of International Money and Finance*, Volume 31, Número 3, Abril 2012, p. 593-605.

WEBGRAFIA

- Baxter, Christian (2017), The Bitcoin Game Theory. Disponível em:
<https://medium.com/@cbaxter/the-bitcoin-game-theory-878b6f479a0b>
- Boettke, Peter (n/d), Austrian School of Economics, *Concise Encyclopedia of Economics*, in The Library of Economics and Liberty. Disponível em:
<http://www.econlib.org/library/Enc/AustrianSchoolofEconomics.html>
- Boston Consulting Group (2017), *Data-Driven Transformation: Accelerate At Scale Now*. Disponível em:
<https://www.bcg.com/publications/2017/digital-transformation-transformation-data-driven-transformation.aspx>
- Buterin, Vitalik (2014), *On mining*, Disponível em:
<https://bitcoinmagazine.com/articles/mining-2-1403298609/>
- Courtois, Nicolas e Bahack, Lear (2014), On subversive miner strategies and block withholding attack in bitcoin digital currency, arXiv:1402.1718v5 [cs.CR]
- Cummings, Dan (2017), *How does centralization place blockchains at risk?* Disponível em:
<https://www.ethnews.com/how-does-centralization-place-blockchains-at-risk>
- Faggart, Evan (2015), *The economics of bitcoin mining centralization*. Disponível em:
<http://bitcoinist.com/bitcoin-mining-centralization-economics/>
- Guadamuz, Andres e Marsden, Chris (2014), *Bitcoin: The wrong implementation of the right idea at the right time*. Disponível em:

SSRN: <https://ssrn.com/abstract=2526736> e <http://dx.doi.org/10.2139/ssrn.2526736>

- Gwartney, James (n/d), Supply-Side Economics, *Concise Encyclopedia of Economics*, in The Library of Economics and Liberty. Disponível em:
<http://www.econlib.org/library/Enc/SupplySideEconomics.html>
- Hanley, Brian (2015), *The false premises and promises of bitcoin*, arXiv: 1312.2048v7 [cs.CE]
- House of Commons (2016) *The digital economy*, Business, Innovation and Skills Committee - Second Report of Session 2016–17. Disponível em:
<https://www.publications.parliament.uk/pa/cm201617/cmselect/cmbis/87/87.pdf>
- McCallum, Bennett (n/d), Monetarism, *Concise Encyclopedia of Economics*, in The Library of Economics and Liberty. Disponível em:
<http://www.econlib.org/library/Enc/Monetarism.html>
- McKinsey Global Institute (2016), *Digital Globalization: The New Era of Global Flows*. Disponível em:
<http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows>
- Nakamoto, Satoshi (2008), *Bitcoin: A peer-to-peer eletronic cash system*, *Cryptography Mailing List*. Disponível em <https://bitcoin.org/bitcoin.pdf>
- OCDE (2012), *The Digital Economy*, Competition Committee Hearings. Disponível em:
<http://www.oecd.org/daf/competition/The-Digital-Economy-2012.pdf>
- Roth, Felix (2009), *The effects of the financial crisis on systemic trust*, Centre for European Policy Studies Working Document n.º 316. Disponível em:
<https://ssrn.com/abstract=1438510> ou <http://dx.doi.org/10.2139/ssrn.1438510>
- Shin, Laura (2017), *Why bitcoin's greatest asset could also spell its doom*. Disponível em:
<https://www.forbes.com/sites/laurashin/2017/04/20/why-bitcoins-greatest-asset-could-also-spell-its-doom/#4b2268ca6adc>