Instituto Superior de Gestão

BITCOIN:
As inconsistências do modelo.

Guilherme Canedo Correia

Dissertação apresentada no Instituto Superior de Gestão para obtenção do Grau de Mestre em Estratégias de Investimento e Internacionalização.

Orientador: Professor Doutor Rui Moreira de Carvalho
Co-orientador: Mestre Joana Paulo Frazão

Lisboa

Junho 2017

I. RESUMO

Com a presente dissertação pretendemos fazer uma revisão de literatura sobre o Bitcoin, assim como confrontar os objectivos que orientaram o desenho do seu protocolo com as evidências sobre o seu funcionamento.

A tecnologia Bitcoin, apresentada por "Nakamoto", em 2008, em plena crise financeira, pretendeu ser, desde a origem, uma alternativa ao sistema financeiro vigente caracterizado pela frágil confiança nos seus principais agentes (v.g., instituições financeiras). A configuração trilateral, paradigmática das transações financeiras, leva a um aumento dos custos de transação (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).

Um sistema de pagamentos *online* alternativo, baseado em código criptográfico e informático, mediante o qual seria possível substituir os intermediários de confiança por uma confiança no código matemático, era um propósito enunciado. Por outro lado, e posto que as transações realizadas 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.

Pretendeu-se, assim, desenvolver um sistema que descentralizado e acessível a qualquer pessoa: disso fez depender, inclusivamente, a segurança do próprio sistema – designado por *Blockchain*. Não obstante, a arquitetura do sistema, a sua complexidade e as "dinâmicas próprias do capitalismo" parecem estimular a centralização na rede do sistema Bitcoin. Assim, a revisão de bibliografia sugere que existem vários níveis de centralização no sistema.

"Nakamoto" limitou a oferta monetária, num total de 21 milhões de unidades de *bitcoins* a atingir em 2140. A oferta fixa e predefinida sugere uma natureza deflacionária do Bitcoin, o que leva muitas pessoas a comprar Bitcoins como um instrumento financeiro, aguardando a sua futura valorização. Este facto tende a dificultar a sua adoção como instrumento de troca.

Como pistas para investigação futura sugerimos (i) estudar a adesão e receptividade da tecnologia Bitcoin em Portugal, (ii) comparar as várias manifestações de tecnologias descentralizadas, e (iii) estudar o funcionamento e dinâmica das plataformas que permitem a realização e execução de *smart contracts*.

PALAVRAS-CHAVE:

BITCOIN, BLOCKCHAIN, MINERAÇÃO, DESCENTRALIZAÇÃO, MOEDA

II. ABSTRACT

With the current dissertation we aim to make a literature review about Bitcoin and to confront the objectives that guided ”Nakamoto”, in the protocol design, with the evidences of its functioning.

Bitcoin technology, presented by Nakamoto in 2008, during the financial crisis, aimed to be an alternative to the current financial system, characterised by the low confidence on its main agents (*v.g*., the financial institutions). The 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.

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

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

Furthermore, "Nakamoto" introduced a limit to the monetary supply, in a total of 21 million *bitcoins*, to be achieved by 2140. This deflationary nature, leads numerous people into buying bitcoins as a financial investment, hoarding them, for future profit. This makes it difficult for Bitcoin to be regarded as a means of exchange.

As clues for future research we suggest (i) studying Bitcoin's adoption and receptivity in Portugal, (ii) comparing different examples of decentralized technologies, and (iii) studying the functioning and the dynamic of *smart contracts'* platforms.

KEY WORDS:

BITCOIN, BLOCKCHAIN, MINING, DECENTRALIZATION, MONEY

III. ÍNDICE

IV. ÍNDICE DE FIGURAS

V. ÍNDICE DE QUADROS

VI. ÍNDICE DE GRÁFICOS

VII. GLOSSÁRIO

51% Attack – ataque informático que pressupõe uma força computacional (*hashing power*) superior a 51% da força computacional existente na rede Bitcoin. O ataque pode assumir várias formas, nomeadamente, alteração do Blockchain, recusa de determinadas transacções, isolamento de determinados *nós* (mineiros).

Bitcoin – uma criptomoeda criada por Nakamoto, em 2008; é o primeiro exemplo de tecnologias descentralizadas, baseadas em prova criptográfica.

Bifurcação (fork) – existência de dois Blochchains; decorre do facto de dois mineiros encontrarem simultaneamente a solução para o puzzle criptográfico, comunicando um novo bloco à rede Bitcoin, para ser adicionado de transacções ao Blockchain. Dependendo das ligações existentes na rede, poderá haver mineiros a "trabalhar" em Blockchains diferentes, problema normalmente resolvido no espaço de horas, mediante votação da própria rede Bitcoin.

Bloco – conjunto de transacções; os blocos são adicionados a cada 10 minutos (em média), pelos mineiros, mediante comunicação à rede Bitcoin.

Blockchain – conjunto de blocos de transacções; contém todo o histórico de transacções realizadas no sistema Bitcoin (uma espécie de livro-razão – *ledger*).

BTC – código monetário das unidades de conta do sistema Bitcoin.

Carteira (*wallet*) – instrumento para guardar as chaves públicas e privadas que permitem a movimentação dos bitcoins. Normalmente, esta funcionalidade é explorada por prestadores de serviços (intermediários), que facilitam a interacção dos utilizadores com o sistema Bitcoin.

Chave (pública e privada) – encriptação própria do sistema; a chave pública é um endereço onde se encontra determinado valor em *bitcoins*, que o respectivo titular pode utilizar (transferir), autenticando a mensagem de transferência desse valor para outro destinatário, com a chave privada. Analogicamente, podemos dizer que a chave pública é uma conta e a chave privada a palavra-chave (*password*) que permite acesso a essa conta.

***Credit crunch* –** contracção dos níveis de crédito concedido pelas instituições financeiras, usualmente, no seguimento de uma crise.

Criptografia – campo da matemática que estuda a encriptação de mensagens, mediante algoritmos.

Criptomoeda – moeda virtual que assenta na encriptação como forma de protecção e segurança.

***Crowd-funding* –** financiamento com recurso ao público em geral; método de financiamento muito divulgado com a internet e o aparecimento das plataformas informáticas.

***Cypherpunk* –** movimento social de matemáticos ativistas, interessados na criptografia, que desenvolveram ferramentas de encriptação, promovendo a liberdade na internet.

***Developers* –** grupo de programadores escolhidos por Nakamoto para introduzirem alterações ao protocolo Bitcoin.

***Digital natives* –** geração social nascida depois do advento das tecnologias digitais.

Gasto duplo – possibilidade de contrafacção de moedas, permitindo a utilização de uma moeda mais do que uma vez.

***Hashing power* –** poder computacional que se traduz na capacidade de transformar uma mensagem num código mais curto ou numa chave. É uma forma de encriptação.

Mineração – função do sistema Bitcoin mediante a qual os *nós* do sistema (os mineiros) resolvem os puzzles criptográficos (com as suas competências e poder *hash*), adicionando transacções a um bloco. É com a publicação do novo bloco na rede que são gerados novos *bitcoins* (novos endereços ou chaves públicas, na verdade).

Mineiro – um tipo de nó da rede Bitcoin que executa o protocolo para criação de novos blocos de transacções. A actividade pode ser prosseguida por particulares ou empresas, mas o acto em si é realizado por *softwares* e *hardwares*.

***Non-banks* –** entidades que não se subsumem à qualificação de bancos/instituições financeiras mas prestam serviços funcionalmente equivalentes aos serviços financeiros.

***Onion routing* –** *software* que permite esconder ligações na internet, mediante redireccionamento destas ligações, em várias camadas.

***Open source* –** diz-se do *software* cujo código (a programação) é livremente acessível, consultável, e replicável pelos interessados. Um *software open source* é também facilmente adaptável a necessidades distintas.

***Peer-to-peer* –** entre pares, ou *nós*; uma rede *peer-to-peer* é uma rede descentralizada em que os intervenientes comunicam directamente entre si, sem necessidade de intermediários.

***Pool* de Mineiros –** associação de intervenientes que executam o protocolo Bitcoin, na mineração de *bitcoins*; a existência destas associações de mineiros resulta da necessidade de reduzir a variância do retorno do investimento, permitindo economias de escala; levam a uma grande centralização na rede Bitcoin.

***Proof-of-work* –** trabalho criptográfico necessário à criação dos blocos, que requer a função *hash*; o trabalho é difícil de conseguir (daí que a atribuição de novos *bitcoins* – o incentivo económico à actividade de mineração – funcione como uma espécie de lotaria) mas fácil de verificar pelos demais intervenientes (que são chamados a votar sobre a validade da criação do novo bloco).

***Rating* –** avaliação financeira.

***Reference client* –** *nó* da rede Bitcoin que executa todas as funcionalidades possíveis na rede.

***Router* –** computador responsável pela gestão e direcionamento do tráfego na internet.

***Shadow banking* –** sistema assente em intermediários financeiros, criados pelos bancos e outras instituições financeiras, que facilitam a criação e concessão de crédito, não se encontrando abrangidos pelo mesmo tipo de regulação e supervisão; por outro lado, este sistema ajudou a ocultar/reduzir o risco assumido pelos bancos e outras instituições financeiras.

***Smart contracts* –** contrato escrito em código capaz de se executar a si próprio, sem intervenção dos contraentes, de acordo com as condições acordadas.

***Stratum* –** protocolo alternativo executado na rede Bitcoin.

***Tainted coins* –** *bitcoins* (na realidade, chaves públicas ou endereços) marcados como ilegítimos ou de qualquer outra forma não merecedores de valor; só os *developers* podem difundir pele rede Bitcoin informação sobre *bitcoins* ilegítimas (adquiridas de forma ilegítima), advertindo toda a rede a não aceitar pagamentos com esses endereços.

VIII. LISTA DE ACRÓNIMOS

AML – *Anti-Money Laudering*

ASIC – *Application Specific Integrated Circuits*

BCE – Banco Central Europeu

IP – *internet protocol*

KYC – *Know Your Customer*

NRI - *Networked Readiness Index*

TOR – *The Onion Router*

1. INTRODUÇÃO

O objecto de estudo é a denominada moeda digital Bitcoin, em geral, e, em particular, as dinâmicas específicas do seu sistema – o denominado Blockchain. Uma das nossas fontes primárias mais importantes, no sentido que lhes atribui Eco (1984, 65-66), é o documento em que tal sistema foi primeiramente apresentado: *Bitcoin: A peer-to-peer eletronic cash system*, publicado em 2008, assinado por Satoshi Nakamoto (cuja verdadeira identidade ainda é 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. Para Ulrich (2014, 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 fenômeno 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, 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. Refere ainda que o sistema actual não é compaginável com pagamentos irreversíveis (ou seja, as transacções são reversíveis em determinadas circunstâncias), facto que promove um acentuar da função de mediação das instituições financeiras (Nakamoto, 2008, 1).

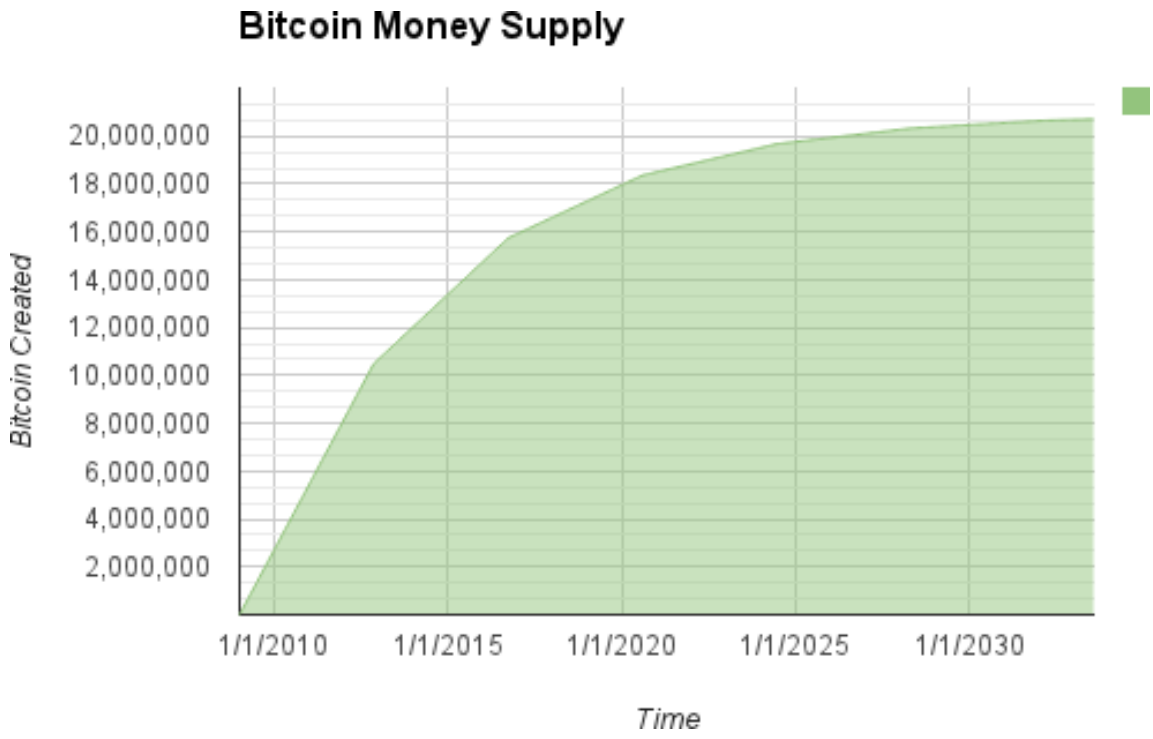
Ora, esta função mediadora implica um aumento dos custos de transacção (Coase, 1937; Williamson, 1975) e generaliza a necessidade de confiança, em especial a confiança nos intermediários, bem como a necessidade de informação pessoal dos agentes económicos (que, de outra forma, não seria necessária) (Nakamoto, 2008, 1).

Nakamoto sugere, então, um sistema de pagamentos electrónico, baseado na criptografia (como suporte da confiança) e não na "clássica" confiança em instituições, que permita aos utilizadores transacionar valor directamente entre si – sem a necessidade de um intermediário de confiança (Nakamoto, 2008, 1). Trata-se de um sistema de pagamentos *online* entre pares (*peer-to-peer*), que utiliza uma unidade de conta própria (os *bitcoins*), e que torna redundante a intermediação de instituições financeiras.

Para Nakamoto o sistema apresentado é uma solução para o problema do gasto duplo (*double-spending*; o gasto duplo foi um problema que atingiu anteriores tentativas de criação de dinheiro digital, e materializa-se na facilidade de duplicação das unidades monetárias), mediante a implementação de um "peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions." (Nakamoto, 2008, 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, que o sistema Bitcoin foi concebido com um número limitado e predefinido de unidades monetárias (Nakamoto, 2008, 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, 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.

Como resulta da curva descrita no Gráfico 1, a oferta monetária vai decrescendo ao longo do tempo. Com efeito, o protocolo Bitcoin prevê que a emissão monetária vá diminuindo para metade, em intervalos de tempo predeterminados de tempo: nos primeiros 210.000 blocos, ou seja, aproximadamente nos primeiros 4 anos (até 2012), por cada novo bloco adicionado à cadeia de blocos (de transacções; o Blockchain) eram geradas 50 unidades monetárias; posteriormente, nos 210.000 blocos seguintes (sensivelmente de 2012 até 2016), por cada novo bloco adicionado ao Blockchain eram geradas 25 unidades monetárias; depois, entre 2016 e 2020, por cada novo bloco adicionado ao Blockchain são geradas 12,5 unidades monetárias; e assim sucessivamente até que seja gerada a última unidade monetária, o que ocorrerá por volta do ano 2140 (Antonopoulos, 2014, 174; Nakamoto, 2009, *apud* Champagne, 2014, 91).

Acrescentamos, ainda, e seguindo Mougayar (2016, 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, 44), "a melhor forma de planear 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 o confronto entre a ideia do sistema Bitcoin com a realidade prática que se tem verificado neste sistema. Com efeito, em 2008, Nakamoto (2008, p. 1) apresentou um sistema de pagamentos *online* descentralizado, no qual circula uma unidade de conta própria. 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 instrumento financeiro, naquilo que, vulgarmente, designamos de "especulação", mais do que como instrumento de troca de um particular sistema de pagamentos. Esta ideia tem sido

sustentada, entre outros, por Guadamuz e Marsden (2014), Hanley (2015), Wu e Pandey (2014), Baek e Elbeck (2014).

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

Q1: O modo de funcionamento (a prática) do sistema Bitcoin tende a traduzir o objectivo (a ideia) da sua criação?

Considerando a natureza dual do Bitcoin, que desempenha uma função de sistema de pagamentos e outra enquanto moeda (Tasca, 2016), julgamos adequado 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, 34-43), permitindo, assim, definir os instrumentos de análise (sejam qualitativos e/ou quantitativos) de forma adequada às respostas que se procuram.

Neste sentido, elencamos as seguintes questões de investigação (Q2 e Q3), enquanto subdivisões da pergunta de partida (Q1):

Q2: O sistema Bitcoin é descentralizado?

Propomo-nos indagar (Q2) o funcionamento do sistema Bitcoin e do seu ecossistema, o modelo de interacção entre os seus intervenientes, as regras de governo e decisão dentro do sistema, bem como, aferir a forma como o poder se encontra distribuído. Recordamos que Nakamoto pretendeu criar um sistema de pagamentos descentralizado, ou seja, um sistema gerido e executado por todos os intervenientes, sem pontos centralizados de poder.

Acresce que a descentralização é uma condição de segurança do próprio sistema, razão pela qual, o grau de descentralização deste poderá ter impacto no grau de confiança depositado pela sociedade (neste tecnologia alternativa) e na sua reputação junto dos utilizadores.

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

Relativamente a esta 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 esclarecer se o facto de se tratar de uma moeda com uma oferta limitada e predefinida (21 mil milhões de unidades, até ao ano 2140) terá algum impacto no comportamento dos utilizadores.

Com efeito, e como adiante se verá de forma desenvolvida, a unidade monetária do sistema Bitcoin pode uma natureza deflacionária, na medida em que a oferta monetária é limitada e pré-definida, podendo originar um desajuste entre a oferta e a procura monetárias. Tal desajuste poderá provocar uma apreciação do valor comparativo desta unidade monetária, o que poderá incentivar a não utilização das unidades monetárias pelos utilizadores. Rogoff (2016, 291) contrapõe sugerindo que o facto de o Bitcoin ser um código aberto, de livre acesso, reproduzível e adaptável, poderá levar à inflação, decorrente da existência de muitas moedas digitais.

1.2 Motivações

A motivação que nos levou à escolha do presente tema prende-se com o desejo de compreensão da tecnologia Bitcoin e dos seus impactos na sociedade.

O potencial desta nova tecnologia (nomeadamente, no que respeita à sua capacidade de desintermediação da sociedade, ou seja, de tornar redundantes os intermediários) tem levado autores como Ross (2016, 89) a questionar se "existe um algoritmo para a confiança" 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." Também Tapscott e Tapscott (2016, p. 5-6) referem que, actualmente, muitas pessoas estão a "tentar perceber as implicações de um protocolo que permite aos meros mortais produzir confiança através de um código inteligente.", o que os leva a designar o protocolo do Bitcoin como o "Protocolo da Confiança".

Para Ross, (2016, 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, 112) reconhece que "A bitcoin encapsula muitas das contradições e possibilidades das moedas digitais, num mundo que se define maioritariamente pelas economias e pelos governos nacionais." Neste sentido, acreditamos que o estudo do sistema Bitcoin permitirá evidenciar estas contradições.

Tapscott e Tapscott (2016, 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 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, tende a desencadear inúmeras novas aplicações e capacidades ainda não realizadas, passíveis de transformar muitas coisas."

Também focado na tecnologia subjacente ao Bitcoin, Mougayar (2016, 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."

Considerando a juventude desta tecnologia, acreditamos que a maioria dos agentes económicos ainda não está familiarizada com o tema (Vigna & Casey, 2016, 3-4). Importa, portanto, desmistificar a tecnologia Bitcoin; criar conhecimento em nome do desenvolvimento. Seguindo Carvalho (2011, 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, genericamente podemos dizer que pretendemos aprofundar o conhecimento da tecnologia Bitcoin, e do seu contexto social e económico. Por outro lado, pretendemos também construir uma narrativa crítica relativamente à arquitectura do sistema Bitcoin e relações de poder no seu seio, bem como, relativamente ao comportamento dos agentes económicos no que se prende com a utilização das unidades monetárias.

1.3. Metodologia

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 narrativa (Green, Johnson e Adams, 2006, 103; Ferrari, 2015, 230-231) como instrumento de investigação.

De forma sucinta, o processo de investigação consiste numa análise crítica e objetiva da literatura existente sobre objecto de estudo. Conforme referem Green, Johnson e Adams (2006, 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. Em suma, é nossa pretensão sintetizar, comparar e contrastar as várias perspectivas sobre o objecto de estudo, num todo coerente (Roberts, 2010, 100).

Esta dissertação resulta, em grande medida, da análise de 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 diversas 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, 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 respeitará a seguinte estrutura: no segundo capítulo, procederemos ao enquadramento do tema, com especial enfoque em conceitos como (i) 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), (ii) a *moeda* e a sua relação com o Estado (em virtude de o Bitcoin ser, também, uma moeda digital), (iii) 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, (iv) 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.

No terceiro capítulo, versaremos o Bitcoin e o seu ecossistema, apresentando as características do sistema e da moeda digital e os estudos feitos sobre o tema. Começaremos pelos antecedentes do Bitcoin, onde a nossa preocupação será evidenciar as tentativas prévias de criação de dinheiro virtual, bem como, os seus contributos para o sucesso do Bitcoin. De seguida, abordaremos, de forma mais profunda, o sistema Bitcoin, na tentativa de evidenciar as suas características. Posteriormente, caberá uma exposição relativa aos aspectos positivos e negativos do Bitcoin. Por fim, importará também detalhar a forma como as instituições governamentais encaram o sistema Bitcoin (particularmente, a nível europeu) e como pretendem regular esta tecnologia.

No quarto capítulo, procedemos à confrontação entre os objectivos da criação do Bitcoin (sistema de pagamentos descentralizado e moeda digital) e a realidade do seu funcionamento. Seguiremos aqui 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, 1)); depois, num segundo momento,

relativamente ao Bitcoin enquanto moeda digital, tentaremos discernir se cumpre a função de moeda e se a arquitectura do seu sistema induz uma utilização como instrumento 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, dando resposta tanto à pergunta de partida como às questões de investigação, e enunciaremos as linhas mestras de investigação futura.

2. ENQUADRAMENTO DO TEMA

Com o presente capítulo, é nosso objectivo conferir ao 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, 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, xxii) identifica três vagas da evolução da humanidade, divisão que permite, segundo o mesmo autor, ter uma melhor visão de conjunto (Toffler,1980, xx e xxii) refere-se a "sínteses de larga escala"): 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, 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.

Toffler (1980, 128-130) distingue as indústrias da segunda vaga (carvão, caminhos-de-ferro, aço, entre outras) – baseadas em princípios eletromecânicos simples, elevados gastos energéticos, desperdício e poluição, trabalho pouco qualificado e repetitivo, bens estandardizados e controlos centralizados – das indústrias da terceira vaga (computação e processamento, aeroespacial, petroquímica, dos semicondutores, das 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, 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 transições[1]. 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 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."

[1] 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, 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, 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.

Por outro lado, Drucker (2007, 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, 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, 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). Conclui Drucker que "Uma disciplina converte um "ofício" em metodologia (…). Cada uma destas metodologias transforma a experiência *ad hoc* em sistema. Cada uma converte o episódico em informação. Cada uma converte a técnica em algo que pode ser ensinado e compreendido." (Drucker, 2007, 59).

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, 1-7) a acreditar que estamos a assistir ao início de uma quarta revolução industrial, marcada pelo advento das tecnologias digitais, a qual implica, em seu entendimento, uma mudança de paradigma social, 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 âmbito.

Também neste sentido, Innerarity (2011, 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" (idem, 30), já que, não existindo, no horizonte temporal, o longo prazo, se perde o espaço da estratégia ("transformam a acção pública em reacção pública").

Castells (2002, 28-29 e 70-72) considera, na linha das investigações de Carlota Perez, Christopher Freeman e Giovani Dosi (que adaptaram ao campo económico, a análise das revoluções científicas, de Thomas Kuhn[2]) que as novas tecnologias[3], especialmente as desenvolvidas a partir da década de 60, do século XX, encerram um novo paradigma[4] tecnológico, com as seguintes características: a informação é um bem e as tecnologias actuam sobre informação; os efeitos das novas tecnologias são omnipresentes, afectando todos os aspecto da vida social; a lógica de rede pode ser aplicada a todos os processos e organizações, permitindo crescimentos exponenciais[5]; 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 ao 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 ou sociedade em rede, de Castells; a híper-história, de Floridi; a idade da inteligência em rede, de Tapscott; entre muitas outras descrições ou qualificações. Para Dias (2014, 23), "Comum a todos estes conceitos é o reconhecimento da importância das tecnologias da informação e da

[2] Para Kuhn (2009, 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, Kunh (2009, 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, 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."

[3] A respeito da origem etimológica da palavra tecnologia, ver Cunha (1986, 759 e 480): do grego "téchnê" (arte, habilidade) e "lógos" (palavra, estudo, tratado).

[4] Han (2016, 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, 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 prossumidor (1980, 251).

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

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 humanos[6], criando novos produtos e serviços, novos modelos de organização, novas formas de produção de energia, de comunicação, de modo mais barato, mais eficiente, mais rápido.

Importa recordarmos, aqui, que os recursos são escassos, por natureza, razão pela qual, as pessoas procuram fazer daqueles que têm ao seu dispor, o melhor aproveitamento possível (Bento, 2004, 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, 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, através da eliminação de barreiras ao comércio e aos movimentos de capitais", de pessoas e bens (Bento, 2004, 93). Para Bento (2004, 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, 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, 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

[6] McQuivey (2013, 7) sustenta que as inovações, consideradas de forma isolada, não criam grande valor, até ao momento em que conseguem ser disruptivas.

ou contracção generalizadas na maioria dos sectores da economia." (Samuelson e Nordhaus, 2005, 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 empresário, ou seja, "pela pessoa que inova" (Diniz, 2010, 104). Segundo Diniz (2010, 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" (também neste sentido, Brynjolfsson e Saunders, 2010, x).

Para Schumpeter o progresso tecnológico é um factor decisivo da produtividade e, consequentemente, do sucesso das sociedade e da melhoria do nível de vida das populações. Também Brynjofsson e Saundres (2010, 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 Tapscott (2015, xiii), a cunhar e a desenvolver o conceito de economia digital, logo em 1995. 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, 38-51; Tapscott, 2015, 2-4; Harari, 2017, 436-437; Plassaras 2013, 379; Ayres e Williams, 2003, 317-329).

Para Bheemaiah (2017, 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)[7]. Invoca, para justificar esta observação, a diminuição do custo dos transístores (lei de Moore[8]), que permitiu um grande desenvolvimento da capacidade dos computadores, levando à ubiquidade

[7] 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, 159).

[8] 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 (Brynjolfsson e Saunders, 2010, ix).

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, 70-71; Bheemaiah 2017, 158-159; Langley e Leyshon, 2016, 2).

Não obstante, como reconhecem Tsyganov e Apalkova (2016, 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, 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, 5) concebe a economia digital como mercados assentes em tecnologias digitais, que facilitam o comércio de bens e serviços através do comércio eletrónico.

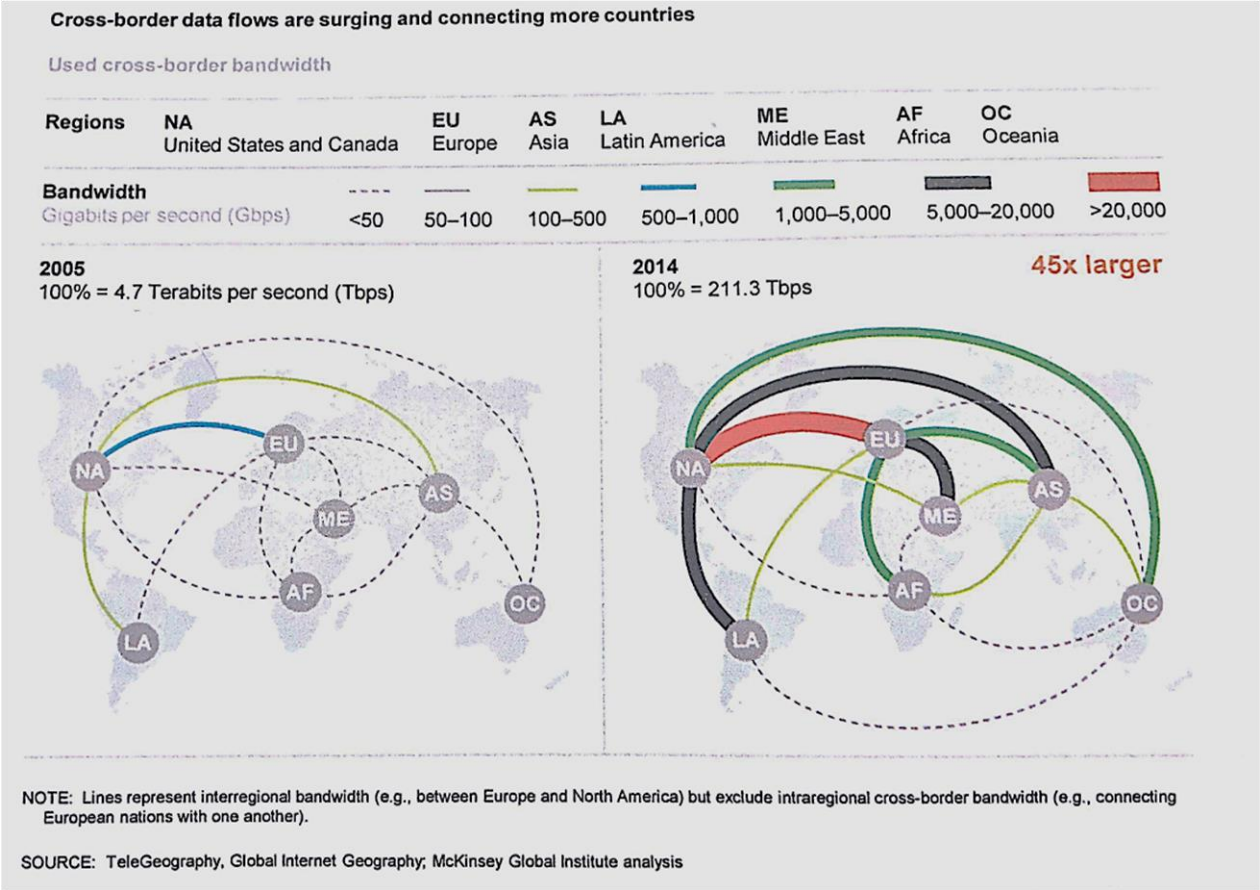
Assim, a economia digital tem por base a utilização das tecnologias da informação e da comunicação, onde se podem incluir, nomeadamente, a internet, a micro-eletrónica, a computação (*hardware* e *software*), as telecomunicações, fibra óptica, comunicação electrónica, comunicação *wireless*, a nanotecnologia, a *Internet of Things* (IoT), a *web* e *web 2.0*, as plataformas digitais, o *cloud computing*, os telemóveis, os *smartphones*, os *tablets*, os écrans 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, 29; Schwab, 2017, 1; Floridi, 2016, vi; Dias, 2014, 24). É a combinação destas tecnologias que leva Schwab (2017, 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 (McMillan, 2014, 125; Tapscott e Tapscott, 2016; Skinner, 2016, 1; Bheemaiah, 2017, 92 e 160).

A nova economia, que é para Castells (2002, 77-78) informacional, global e em rede, assenta num novo conjunto de princípios, como a colaboração, a abertura, a partilha, a interdependência, a integridade (Tapscott, 2015, 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 (Toffler, 1980, 251; Rifkin, 2016; Kotler, Kartajaya e Setiawan, 2017, 27-39; Schultz, 2013, 144; Langley e Leyshon, 2016, 3). Kotler, Kartajaya e Setiawan (2017, 27-39) sublinham, ainda, que "a transferência de poder para os consumidores conectados" assenta em três transições: (i) do vertical para o horizontal (que se pode traduzir num nivelamento do poder e da influência, entre consumidores e empresas); (ii) do exclusivo para o inclusivo (facilidade de acesso a bens e serviços, bem como, menor custo

de diferenciação de produtos a uma escala global); e, (iii) do individual para o social (importância acrescida da opinião dos nossos pares).

Por outro lado, os fluxos digitais que materializam a economia digital estão a alterar, também, a própria estrutura empresarial (Tapscott, 2015, 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, 4) - Figura 1.

Figura 1: aumento dos Fluxos Digitais

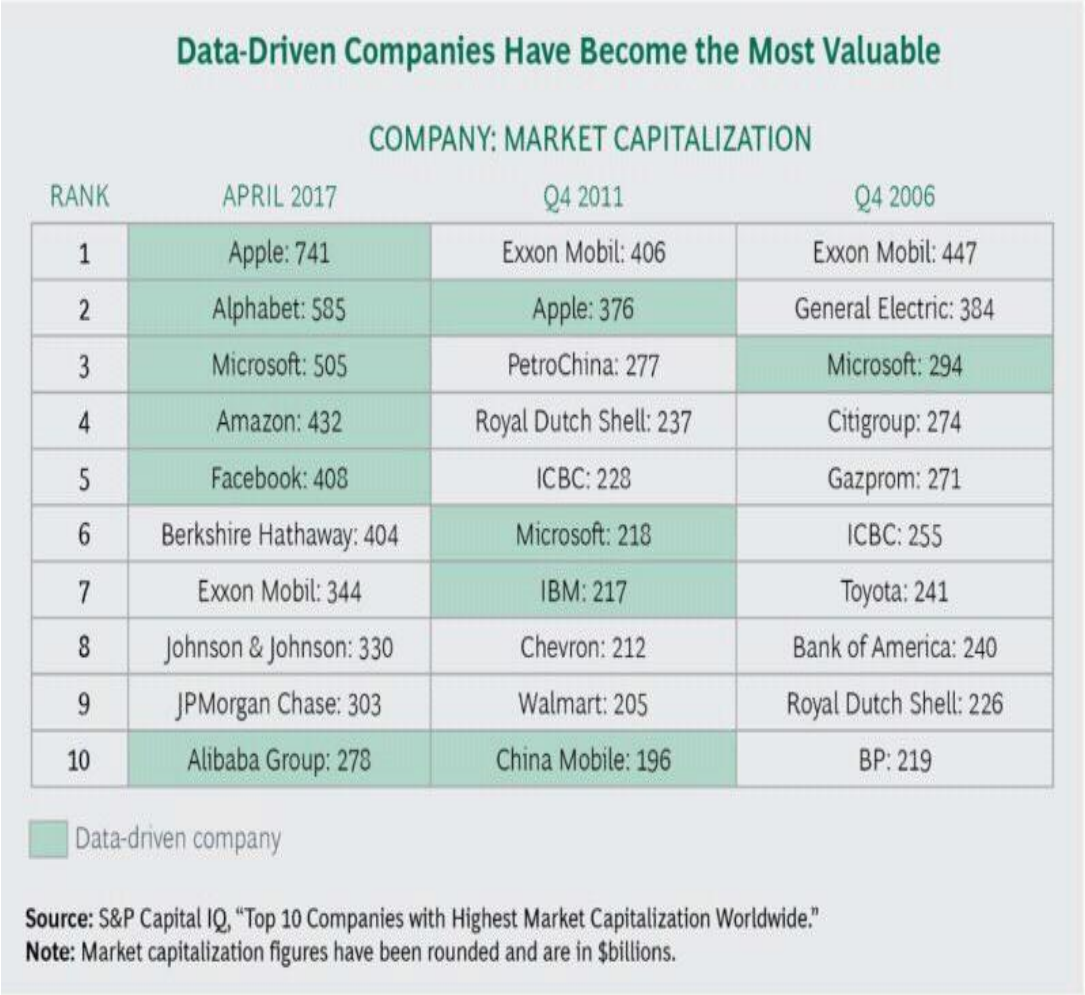


Fonte: Digital Globalization: The New Era of Global Flows, McKinsey Global Institute, 2016.

Na Figura 1 vemos como a largura de banda e os fluxos digitais aumentaram em todo o mundo, entre 2005 e 2014. O volume dos fluxos digitais global aumentou de 4,7 *Terabits* por segundo para 211,3 *Terabits* por segundo (45 vezes superior). O tráfego digital existente entre a América do Norte (NA) e a Europa (EU) destaca-se como sendo o mais volumoso de todos.

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.

Quadro 1: crescimento empresas de base informacional



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.

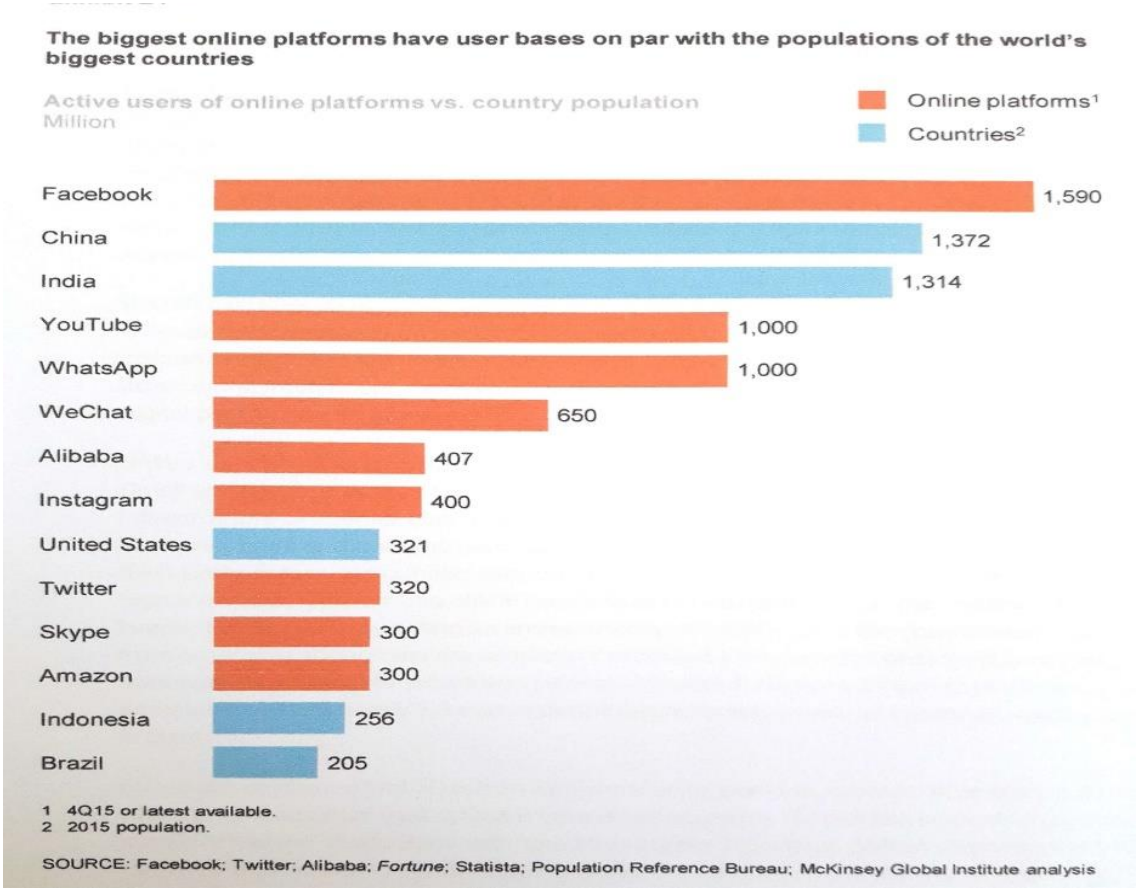
Fonte: Data-Driven Transformation: Accelerate At Scale Now (Boston Consulting Group, 2017

No Quadro 1 percebemos uma predominância das empresas "digitais", ou de base informacional, relativamente aos tradicionais sectores da economia: se em 2006 apenas existia uma empresa digital no top 10 (capitalização bolsista em todo o mundo), em 2017 já 6 das 10 empresas mais valiosas mundialmente são de base informacional. Além desta predominância do sector informacional face a outros sectores, destaca-se também o aumento do valor de cada empresa.

Por fim, e mais recentemente, o surgimento das plataformas digitais intensificou os impactos sociais e económicos da economia digital (McKinsey, 2016, 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 ofereceu 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, 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, 6).

Gráfico 2: dimensão plataformas digitais



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

No Gráfico 2 vemos a dimensão das plataformas digitais, equiparável já à dimensão dos maiores países em termos demográficos. Isto revela a eficácia destas plataformas a agregar utilizadores, bem como o poder (informação) que têm ao seu dispor.

Parker, Alstyne e Choudary (2016, 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 em informação e na promoção e desenvolvimento de comunidades, razão pela qual, é dada especial atenção aos efeitos de rede na criação de eficiências. No entanto, Ross (2016, 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 afastas 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, redireciona 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, xiv), com enorme potencial disruptivo para a sociedade.

2.2. A moeda e o Estado

A invenção da moeda, pelos sumérios, há cerca de 5.000 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 (Ingham, 2004, 3; Ingham, 2016, 67; Harari, 2017, 184-186). Rogoff (2016, 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 preços[9]) (Ingham, 2004, 3-4; Samuelson e Nordhaus, 2005, 513; Daniel, 2013, 125).

[9] O controlo dos preços está, usualmente, associado ao controlo da inflacção (subida geral de preços) e da deflacção (descida geral de preços). Fisher (2015, 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 inflacção ou deflacção *relativas* – pela circulação monetária a ultrapassar a circulação de bens, ou o inverso."

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, 125)[10], antes surgindo delimitado, habitualmente, por referência às suas funções típicas[11]: "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, 125). Autores como Ingham (2004, 3; 2016, 67) e Martin (2013, 39) encaram a moeda, o dinheiro, como uma tecnologia social.

Ingham (2004, 4) destaca ainda, invocando a obra e a 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, 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, 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 seu poder (moedas territoriais) (Cohen, 1998, 32). Este controlo estava intimamente ligado aos sistemas nacionalistas, e o poder resultante derivava do monopólio monetário, mediante quatro canais: (i) simbolismo político (promotor de unidade), (ii) direitos de senhoriagem (e o implícito aumento da oferta monetária, com o objectivo de aumentar a despesa pública), (iii) gestão macroeconómica (com impacto na produção interna e no controlo do desemprego; capacidade para regular as taxas de câmbio, em termos de trocas

[10] 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.

[11] A este respeito, *vide* Fernandes e Mota (2015, 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."

internacionais), e (iv) isolamento monetário (independência monetária e aumento da autoridade estatal) (Cohen, 1998, 35-46).

Cohen (1998, 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 (Cohen, 1998, 150) conclui, observando, que a economia actual, globalizada e interdependente, promoveu o aparecimento de redes impessoais de transação, de troca, que são alheias às fronteias 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, 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."[12] 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, 71)[13].

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, 62). Porém, estas trocas nem sempre se realizaram no âmbito de sistemas monetários. Na verdade, e como referem Fernandes e Mota (2015, 9), "Cronologicamente temos em primeiro lugar as chamadas economias de troca directa que correspondem a um estádio inicial e bastante 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, 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

[12] 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, 87).

[13] 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, 88).

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, 27) seleciona 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, 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 excurso 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, 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." (Friedman, 2014, 72), razão pela qual, este padrão "tem sido acompanhado da criação de vários tipos de dinheiro fiduciário, aparentemente convertível no bem monetário em condições preestabelecidas" (Friedman, 2014, 72). No âmbito deste padrão, "a moeda vale o que valer o seu conteúdo intrínseco." (Fernandes e Mota, 2015, 23).

Fernandes e Mota (2015, 23-34) distinguem os vários momentos do sistema monetário, referindo-se a sistemas não metálicos e a sistemas metálicos (e, dentro destes, aos sistemas monometálicos, aos bimetálicos e ao padrão-ouro) – neste sentido também Silva, Mota, Queirós e Pereira (2013, 52-54). 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." (Fernandes e Mota, 2015, 34).

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, 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 recursos[14]. Neste sentido, Bento (2004, 73) refere que "Teoricamente baseado na voluntária abdicação 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, 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, 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-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, 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, 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.

[14] 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 consumam 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."

Ross (2016, 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, é oportuno 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, 22) que faz a ligação entre o Bitcoin e a escola austríaca (de pensamento económico)[15]: "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 econômicos exacerbados e inflação maciça."

Segundo o Banco Central Europeu (2012, 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 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, 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 inflacção criada pelos governos, numa constante distorção da economia, que só foi possível pelo monopólio da moeda. Por conseguinte, Hayek (1990, 131-133) apresenta um programa, assente

[15] 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."

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 frisar que a associação entre o Bitcoin e a crise financeira é feita pelo próprio criador, Nakamoto, o qual, aquando da criação do Bloco Génese, publicou a seguinte mensagem: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" – uma referência directa aos resgastes bancários com dinheiros públicos. Conforme refere Ulrich (2014, 43), "A alusão à manchete do jornal britânico *The Times* daquele dia não é acidental. 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, 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, 37) reconhece, a respeito da crise de 2008, que a atenção dos analistas e investigadores se tem focado, primacialmente, "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, 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 monetaristas[16] e da economia pelo lado da oferta[17]. Este novo modelo de crescimento

[16] 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).

[17] 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

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, India, 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, 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, Valdez e Molyneux (2010, 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 pelas empresas financeiras, obtidos com suporte em "alavancagem financeira", a política de remunerações incentivadora da tomada de riscos, os distorcidos e desalinhados 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

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).

(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, 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-dívida[18], 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, 2014, 92). Estas injecções 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 injecções de capital, a resposta governativa implicou, também, um aumento de regulação e de supervisão do sector financeiro (McMillan, 2016, 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, 20).

[18] Cfr., a este respeito, Carvalho (2011, 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."

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, 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 & Casey, 2016, 13). Referem estes autores, ainda, que o Bitcoin ofereceu uma alternativa ao sistema financeiro vigente, que estava perto do colapso e que ameaçava arrastar consigo milhões 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, 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, 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 bancária[19].

[19] Também neste sentido, Arvidsson (2014, 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."

Alt e Puschmann (2012, 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, 462-463) argumenta que o campo dos pagamentos[20] 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

A já referida "aceleração da sociedade", provocada pelo progresso tecnológico, é analisada por Innerarity (2011, 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." (*idem*, 35). Este imediatismo, a "cultura da urgência", reduz a capacidade de as sociedades fazerem planos a longo prazo, transformando a política em demagogia (*ibidem*, 40-43; Han, 2016, 29). Neste seguimento, Innerarity (2011, 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."

Sucede que, como refere Finuras (2013, 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."

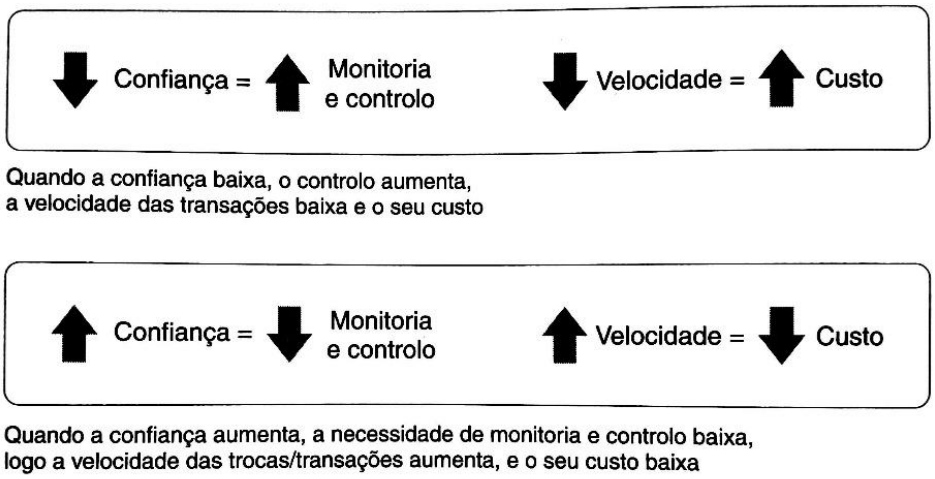
[20] Para Arvidsson (2014, 463), o campo dos pagamentos engloba, por um lado, o sistema de pagamentos, e, por outro, o ambiente que envolve o sistema de pagamentos (incluindo-se aqui os valores sociais, factores económicos, questões políticas, evolução tecnológica, questões ecológicas e legais).

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 (*idem*, 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, 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, 35) refere que "a confiança remete para a coesão social, considerada indispensável ao funcionamento das sociedades modernas, complexas e diferenciadas".

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 inter acções e no chamado «custo das transacções»" (Finuras, 2013, 138). Finuras (2013, 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 monitorização e controlo (que engloba o custo da informação), e diminui a velocidade das transacções, aumentando o seu custo. No Quadro 2, Finuras (2013, 142), esquematiza o impacto da confiança na economia e nas transacções:

Quadro 2: impacto da confiança na economia e nas transacções



Fonte: Finuras, 2013

Ou seja, de acordo com a esquematização apresentada no Quadro 2, a diminuição da confiança entre os agentes económicos tem como consequência uma maior necessidade de controlo, o que afecta negativamente a velocidade do comércio e o custo transacção. O aumento da confiança terá os efeitos contrários, aumentando a velocidade do comércio e afectando positivamente o custo de transacção.

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, 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".

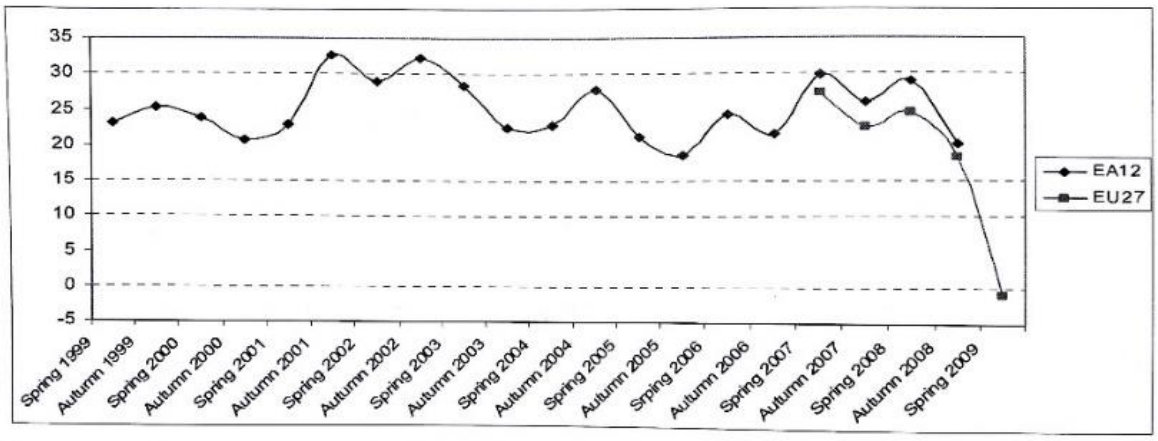
No âmbito do sector financeiro, e especialmente das transacções económicas, o problema da confiança tem sido resolvido mediante a intermediação realizada pelos bancos (e outras instituições financeiras), entre indivíduos e empresas (que não se conhecem), intermediação esta suportada por Bancos Centrais e Entidades Reguladoras, que conferem confiança ao sistema através da supervisão (Adriano e Monroe, 2016, 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, 196), Roth (2009, 1), Walti (2012, 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):

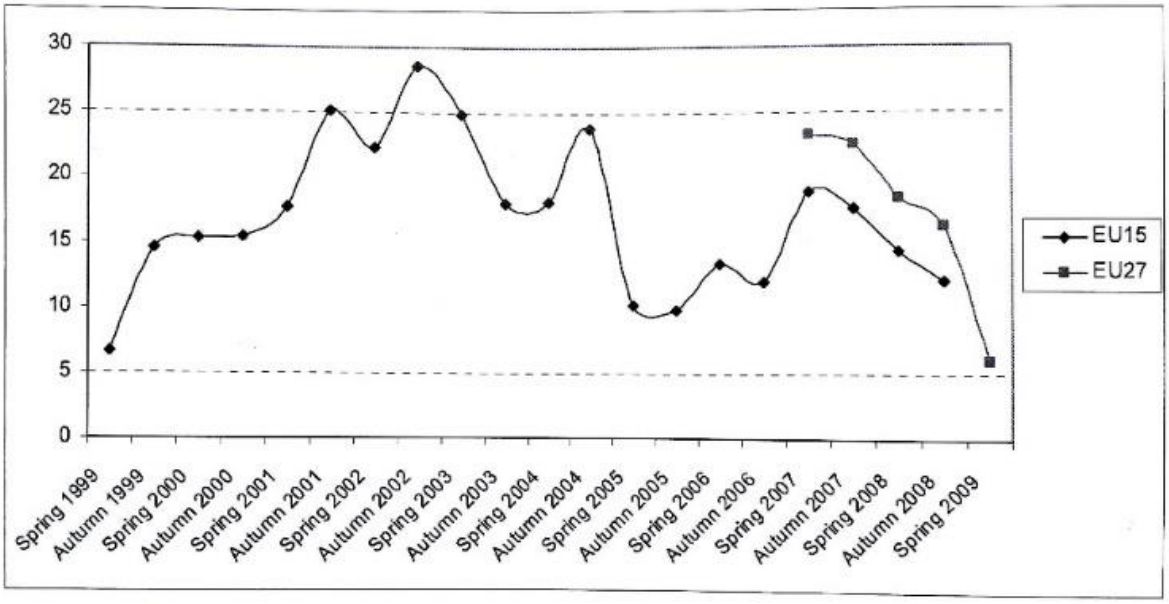
Gráfico 3: evolução da confiança no Banco Central Europeu



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

Fonte: Roth, 2009

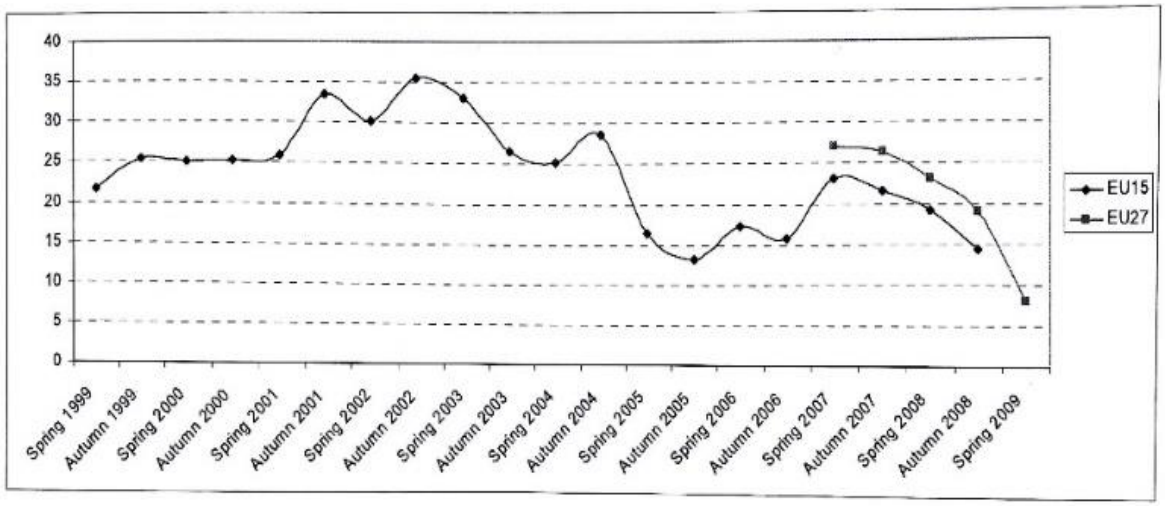
Gráfico 4: evolução da confiança na Comissão Europeia



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

Fonte: Roth, 2009

Gráfico 5: evolução da confiança no Parlamento Europeu



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

Fonte: Roth, 2009

Os Gráficos 3, 4 e 5 são exemplificativos da diminuição da confiança dos cidadãos europeus em três instituições comunitárias (Banco Central Europeu, Comissão Europeia e Parlamento Europeu), entre a Primavera de 1999 e a Primavera de 2009. Apesar de os níveis de confiança nestas instituições nunca terem sido elevados (no período retratado), assiste-se a uma deterioração da confiança a partir da Primavera de 2007, quando começa a crise financeira nos Estados Unidos da América.

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 bancário se encontram, maioritariamente, países europeus onde a crise financeira foi sentida de forma 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, 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, 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 Nakamoto (2008, 1) considerava que o Bitcoin podia ser uma forma de resolver o actual problema de confiança que afecta a sociedade, levando Tapscott (2016, 6), como já referimos, a qualificá-lo como o "Protocolo da Confiança".

É nosso entendimento que as moedas digitais semelhantes ao Bitcoin são um desafio ao surgimento de produtos e tecnologias semelhantes (o que começa a ser já uma realidade), que tenderão a competir com as clássicas moedas fiduciárias.

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

3. BITCOIN

Como referimos na Introdução, Nakamoto (2008, 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: o primeiro (i) refere-se ao sistema ao sistema de pagamentos; o outro, (ii) à unidade de conta – a moeda. Ou seja, tem uma natureza dual (Tasca, 2016; Brito e Castillo, 2016, 7).

A tecnologia Bitcoin é um novo tipo de moeda digital, que circula numa plataforma própria (Tasca, 2016, 68). Para Tapscott (2016), o advento da tecnologia Blockchain permite transformar a "Web da Informação" numa "Web do Valor", e isso poderá trazer algo novo, que assenta, entre outros, nos seguintes pilares: (i) criação de redes *peer-to-peer* assentes em plataformas, promotoras da partilha e da colaboração; (ii) alteração do paradigma financeiro, em nome da inclusão e da velocidade de execução e de acesso; (iii) protecção de direitos de forma globalizada; (iv) eliminação de burocracias e de corrupção (nomeadamente, na ajuda externa a países pobres); (v) valorização do trabalho dos criadores (direitos de autor); (vi) reconfiguração do conceito de empresa enquanto motor do capitalismo (predomínio das plataformas); (vii) alteração das formas de governação.

3.1. Antecedentes do Bitcoin

O Bitcoin, enquanto fenómeno tecnológico, agregou algumas tecnologias preexistentes, e aproveitou o conhecimento gerado por anteriores tentativas de criação de uma moeda digital (Narayanan *et al*, 2016, ix; Rothstein, 2017, 23; Carboni, 2017, 37). Em virtude deste facto, Antonopoulos (2015, 1) considera o Bitcoin "uma coleção de conceitos e de tecnologias que formam a base do ecossistema do dinheiro digital". Mougayar (2016, 10) encara esta nova tecnologia da seguinte forma: "O Blockchain é uma metatecnologia 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, 2017, 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, 2017, 24-26; Vigna & Casey, 2016, 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, 2017, 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, 38).

No entanto, Rothstein (2017, 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 - *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 & Casey (2016, 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" (Vigna & Casey, 2016, 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.

Das várias tentativas anteriores destacamos as seguintes: *DigiCash* (David Chaum, 1989), *hashcash* (Adam Back, 1997), *b-monney* (Wei Dai, 1998), *bit-gold* (Nick Szabo, 1998-2005) (Narayanan *et al*, 2016, 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 (contrafação). Foi este problema que o Bitcoin, mediante a tecnologia Blockchain, veio resolver (Brito & Castillo, 2016, 6).

3.2. O sistema de pagamentos Bitcoin

Olhando o Bitcoin enquanto sistema de pagamentos, importa considerar que o mesmo não é controlado por Estados, por bancos centrais, por entidades governamentais, ou mesmo por bancos ou outras instituições financeiras (Rothstein, 2017, 3). Aliás, e de acordo com a ideia original de Nakamoto, 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, 1).

Para Nakamoto (2008, 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) – que se designa Blockchain. Por fim, a segurança da rede (do sistema) exige que "pelo menos 51% da rede seja honesta" (Nakamoto, 2008).

Para Mougayar (2016, 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, 29-51), focando-se no Blockchain, sustenta que esta nova tecnologia encerra o poder de revolucionar a forma como organizamos a sociedade[21]. São sete os princípios de

[21] Como vimos, Tapscott (2016) 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.

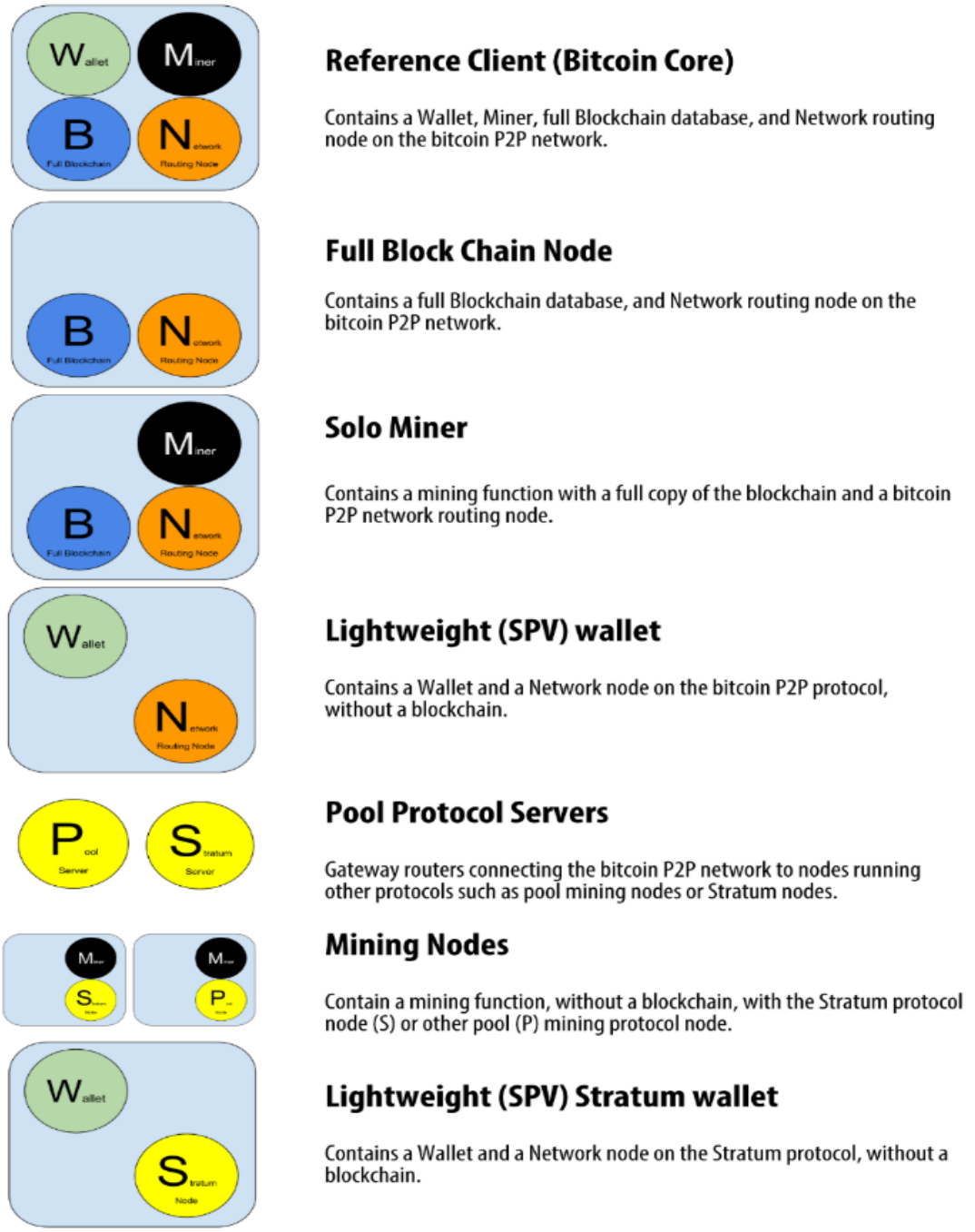
arquitectura que elenca: integridade da rede; poder distribuído; valor como incentivo; segurança; privacidade; garantia de respeito e reconhecimento de direitos; inclusão.

3.2.1. A rede peer-to-peer:

Antonopoulos (2014, 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 semelhantes, 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 (2014), 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, 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. Já na Figura 2 encontramos uma exemplificação da "rede alargada", referida por Antonopoulos (2014, 140).

Quadro 4: tipologia dos nós do sistema Bitcoin

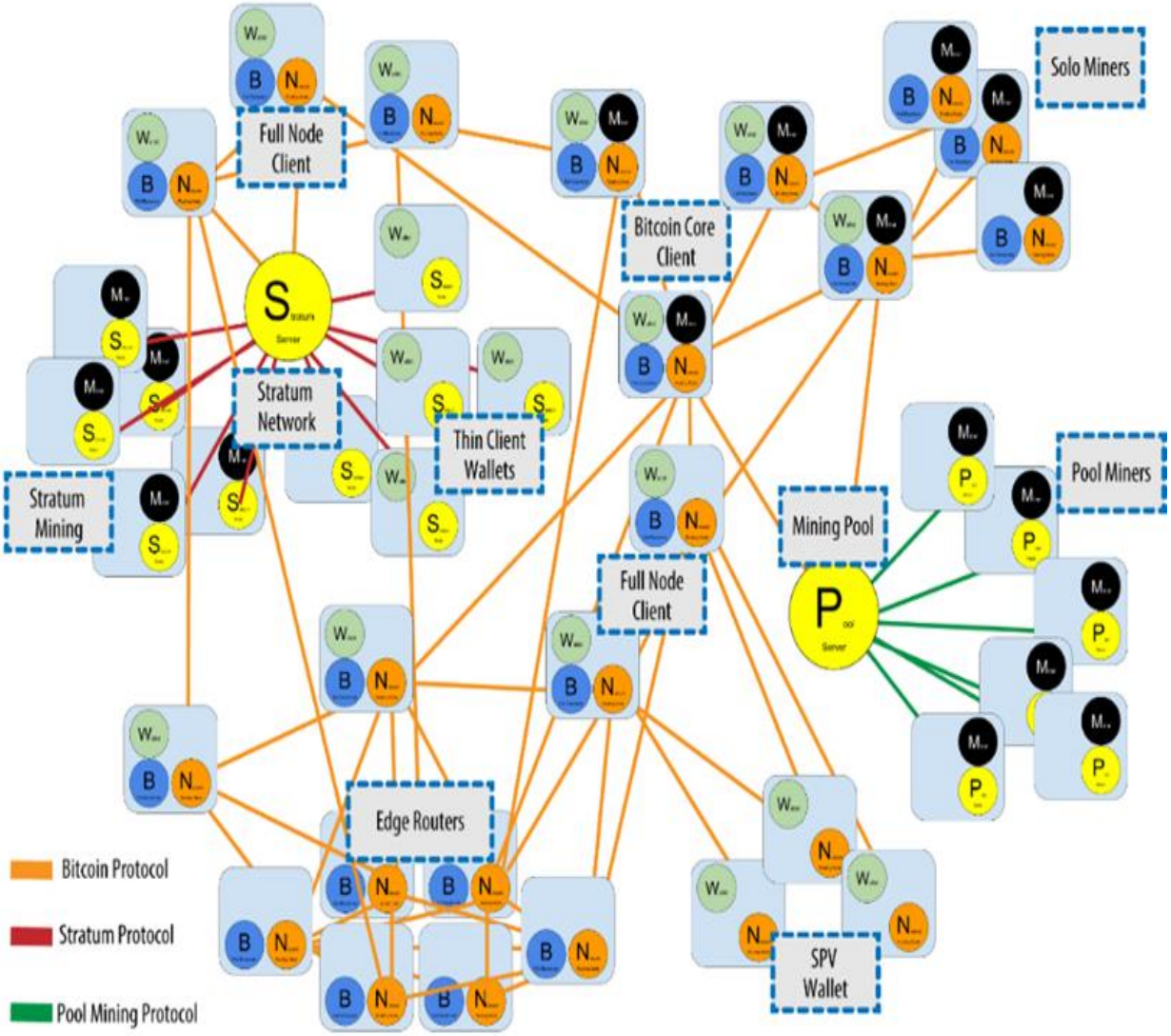


Fonte: Antonopoulos (2014)

No Quadro 4 encontramos os vários tipos de nós que se podem encontrar na rede do sistema Bitcoin. Como resulta deste quadro, nem todos os *nós* desempenham todas as funções necessárias ao sistema. Assim, um nó é designado *Reference Client* quando desempenha todas as funções do sistema: carteira, mineração, base de dados (contém cópia integral do Blockchain)

e *router* do sistema P2P (transmissão/divulgação das mensagens). No entanto, cada interveniente decide que funções pretende desempenhar, estabelecendo parcerias com outros *nós*. Por exemplo, um *Solo Miner* pode querer ter uma cópia completa do Blockchain (o documento que contém todas as transacções desde a origem), ou pode preferir integrar uma Pool de Mineiros, caso em que não terá função de *router* do sistema Bitcoin P2P, uma vez que se ligará apenas à sua Pool, usando para o efeito o protocolo Stratum (ou outro protocolo de transmissão/divulgação de mensagens).

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



Fonte: Antonopoulos (2014)

Na Figura 2 encontramos uma exemplificação da rede alargada do sistema Bitcoin. Como se vê desta construção teórica, os *nós*, além de não desempenharem todos as mesmas funções, e além de não desempenharem todas as funções possíveis, também não estão todos ligados entre si. O

acesso à informação na rede Bitcoin depende das ligações que cada *nó* tenha com outros *nós*. Por exemplo, do lado direito da Figura 2 vemos vários nós Mineiros, que não estão ligados à rede Bitcoin directamente, mas antes ao Router da Pool de Mineiros a que se associaram. Por sua vez, a Pool de Mineiros está ligada a um nó completo, um *Bitcoin Core Client*, de onde recebe informação e para onde envia informação (desde logo, sobre o Blochchain ou, mais especificamente, sobre os novos blocos de transacções).

Da Figura 2 constam também *Solo Miners*, Carteiras (*Wallets*), entre outros tipos de nós, demonstrando a complexidade que esta rede pode assumir. Vemos também que os protocolos usados não são os mesmos em toda a rede.

3.2.2. As transacções e a mineração:

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

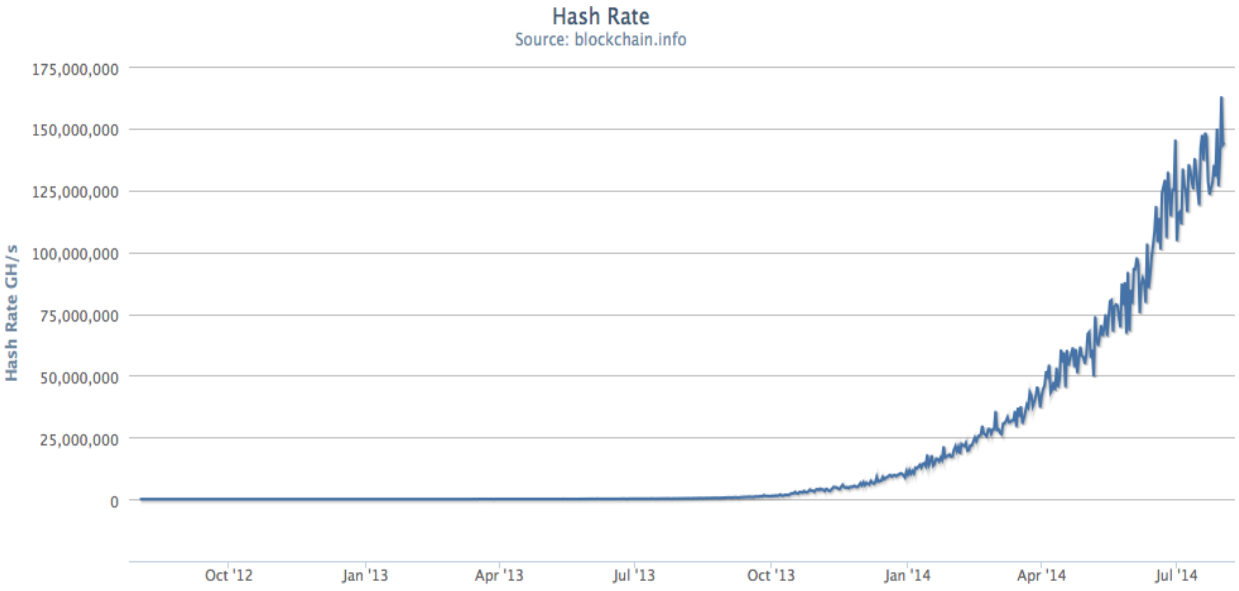
Adicionalmente, para que o bloco seja válido e adicionado ao Blockchain deve satisfazer a condição criptográfica *proof-of-work*, contendo o cabeçalho do boco anterior (também este gerado de forma criptográfica). Esta função criptográfica é de difícil solução (funciona como tentativa e erro), mas fácil 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 pelos mineiros ao Blockchain a cada 10 minutos, correspondentes ao tempo médio que demorará a ser encontrada a solução do puzzle criptográfico. Para que se consiga este tempo médio de criação de novos blocos, o protocolo do Bitcoin vai adaptando a dificuldade do puzzle à capacidade computacional existente na rede (Antonopoulos, 2014, 195): ou seja, quanto maior for a capacidade computacional (mais mineiros) mais difícil será o puzzle. O objectivo é ter uma emissão constante e regular de novas unidades monetárias, tanto a curto como a longo prazo, razão que leva Antonopoulos a considerar que a criação de blocos (e correspondente emissão monetária) é "o batimento cardíaco" do sistema Bitcoin (Antonopoulos, 2014, 195).

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) (Narayanan *et al*, 2016, 117-118). 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 (Narayanan *et al*, 2016, 119) o que impede o acesso de muitos utilizadores ao negócio de mineração.

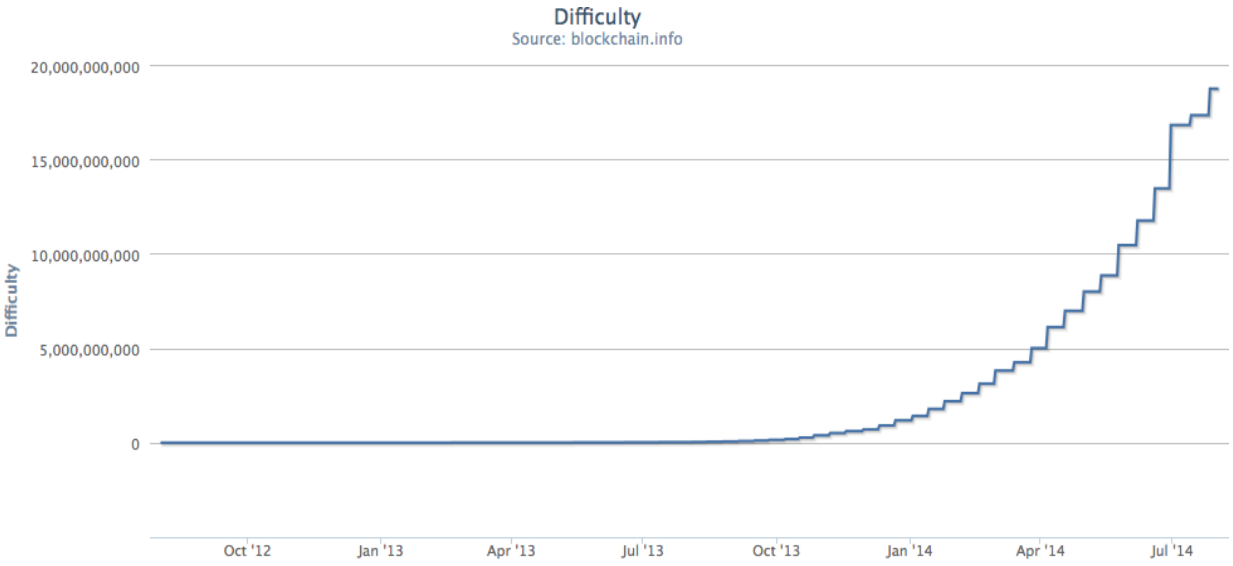
Gráfico 6: evolução do poder de computação



Fonte: Antonopoulos (2014)

O Gráfico 6 demonstra um poder de computação crescente na rede Bitcoin, que resulta não apenas da entrada de novos intervenientes (mais mineiros), mas também da potência computacional de cada interveniente (melhoria do software e do hardware).

Gráfico 7: evolução da dificuldade do puzzle matemático



Fonte: Antonopoulos (2014)

Consequentemente, e como se referiu, a dificuldade do puzzle criptográfico (Gráfico 7) é também crescente: mais mineiros, com maior capacidade computacional (medida através da capacidade *Hash*), fazem com que o grau de dificuldade aumente, para ser mantido o ritmo de 10 minutos de criação de blocos (e correspondente emissão monetária).

Estes factos têm levado muitos mineiros a associarem-se entre si, constituindo as designadas *pools* de mineiros, ou *mining pools* (Narayanan *et al*, 2016, 124; Antonopoulos, 2014, 207).

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

3.3.3. A unidade monetária:

Versando agora o *bitcoin* enquanto moeda, Ross (2016, 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, 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, 7). Aliás, como refere Nakamoto (2014), 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* (unidade monetária) 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. Já o BCE (2015, 23) considera, em sentido contrário, que a fraca aceitação no mercado global dos *bitcoins* permite sustentar que esta unidade monetária não serve como meio de troca.

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 e sustentar que cumpre de forma muito eficaz a função de unidade de conta.

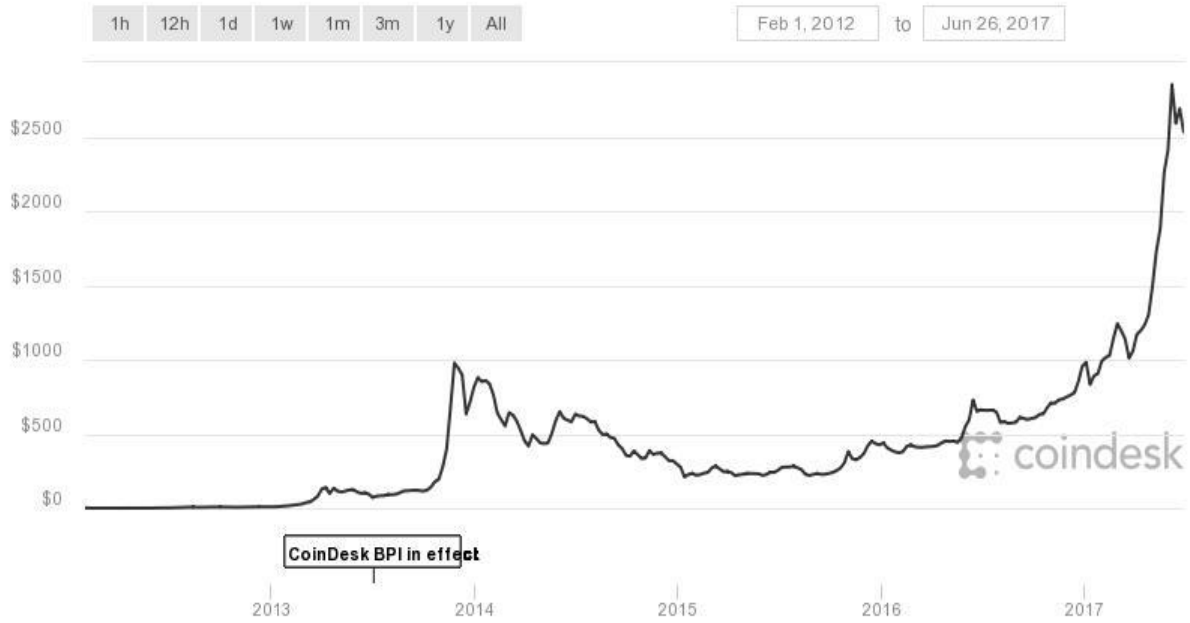
Por fim, enquanto reserva de valor, a natureza deflacionária do inerente ao sistema Bitcoin impede a sua consideração como instrumento de reserva de valor (neste sentido, também, BCE, 2015, 23). Com efeito, e como refere Antonopoulos (2014, 176) o sistema Bitcoin é inerentemente deflacionário, em função da sua oferta monetária ser fixa e pré-definida (vai diminuindo com o tempo). Esta arquitectura monetária, além de resistir a fenómenos artificialmente inflacionários (emissão de moeda não dependente de indicadores económicos reais, ou seja, não correspondente a um desajuste da oferta monetária face à economia real). Por outro lado, esta natureza deflacionária pode originar pouca liquidez monetária, uma vez que os detentores do *bitcoins* tenderão a guardar as suas unidades monetárias, o que provocará,

por sua vez, nova apreciação do valor de troca do *bitcoin*. A falta de liquidez não poderá ser aliviada mediante emissão de novas unidades monetárias.

Esta arquitectura promove uma grande volatilidade no valor de troca da unidade de conta *bitcoin* (a oscilação/variação do valor de troca não encontra comparação com outras moedas ou matérias-primas). 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 financeiro e monetário vigente, em que o valor de uma moeda é condicionado pelos diversos instrumentos monetários). Na verdade, o valor da unidade de conta *bitcoin* 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 um 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, como se viu, da própria configuração do sistema.

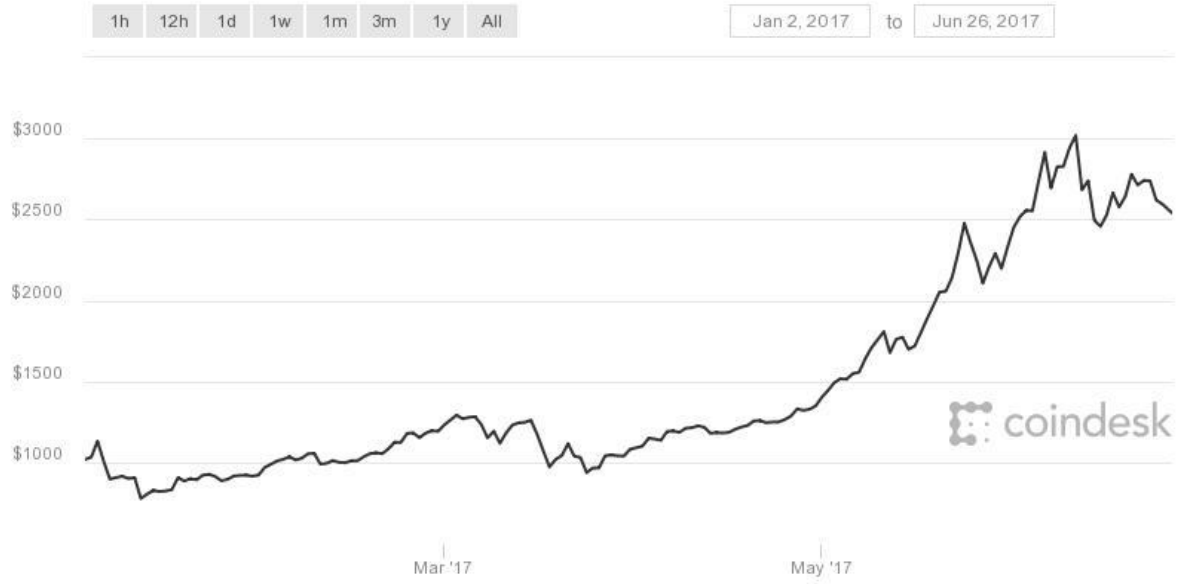
Gráfico 8: valorização no período 2012-02-01 / 2017-06-26



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

(consultado em 2017-06-26)

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



Fonte: http://www.coindesk.com/price/
(consultado em 2017-06-26)

Nos Gráficos 8 e 9 vemos a evolução do câmbio (para dólares americanos) da unidade de conta *bitcoin*: primeiro no período entre 2012-02-01 e 2017-06-26; depois, no período entre 2017-01-02 / 2017-06-26. Estes gráficos são elucidativos das grandes oscilações do valor do *bitcoins*. Por exemplo, de forma significativa podemos dizer que a subida abrupta do valor dos *bitcoins* em 2013 (Gráfico 8) ficou associada à crise financeira e política no Chipre, que originou uma enorme procura (fuga) por uma moeda digital, não apropriável pelos poderes governativos e/ou judiciais. Mais recentemente, a valorização constante dos *bitcoins* parece resultar de um maior conhecimento desta tecnologia, e de uma maior aceitação social e até mesmo por alguns Estados.

3.3. Aspectos positivos, negativos e desafios

A ideia de que a tecnologia Bitcoin é disruptiva é muito veiculada na sociedade, através tanto de especialistas como dos *media* generalistas[22]. 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 (1995), a disrupção começa com soluções mais simples e mais baratas, na base de um mercado ou sector, e que

22

gradualmente vão alargando a sua influência e adopção (movimento *upmarket*), destruindo indústrias estáveis.

Não obstante, e apesar da influência que esta tecnologia pode ter na nossa sociedade, é importante evidenciar as suas características, expondo prós e contras.

3.3.1. Aspectos positivos

Como principais ascpectos positivos apresentamos os seguintes:

(i) Anonimato: O anonimato, ou melhor, a privacidade que o sistema de chaves públicas e privadas permite (é um sistema pseudónimo), 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.

(ii) Redução dos custos de transacção e aumento da velocidade: Para Mougayar (2016, 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.

(iii) Estímulo à inovação financeira e tecnológica: 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 s*mart 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;

(iv) Potencial de redução da pobreza e opressão: O Bitcoin pode, também, 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

Como principais ascpectos positivos apresentamos os seguintes:

(i) Anonimato: Como referimos anteriormente, o sistema Bitcoin não é anónimo mas pseudónimo: as transacções não só são visíveis por todos (transparência absoluta), 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 tanto pode ser um aspecto negativo como positivo: será negativo do ponto de vista das entidades reguladoras, pois fica difícil controlar a actuações criminosas, como por exemplo, a lavagem de dinheiro, a fuga ao fisco, entre outras.

(ii) Volatilidade da moeda: Para o sistema Bitcoin funcionar da forma como foi concebido por Nakamoto, é essencial que as unidades de conta tenham grande circulação. Daí que a enorme volatilidade seja vista como um aspecto negativo, promovendo-se antes uma utilização enquanto instrumento financeiro e não como meio de troca.

(iii) Falhas de segurança: Apesar de o sistema ainda não ter sido violado, já houve várias falhas no ecossistema Bitcoin. Na verdade, os pontos de informação centralizada, como por exemplo, os intermediários, representam o "calcanhar-de-Aquiles" do sistema.

(iv) 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 (alegado) anonimato que permitido aos 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), nomeadamente;

(i) 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), profundos, amplos e complementares. 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;

(ii) Associação à actividade criminosa: Por outro lado, a primeira aplicação da tecnologia Blockchain, o Bitcoin, anda muitas vezes associada à actividade criminosa, o que pode dificultar a sua adopção de modo generalizado;

(iii) 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: (i) Ambiente tecnológico (político, regulatório, empresarial, inovação); (ii) Preparação da rede (infraestrutura TIC, custos, capacidades e competências); (iii) Adopção de tecnologia (empresas, governos, particulares); (iv) Impacto económico e social.

(iv) Capacidade transacional e liquidez: Do ponto de vista do Bitcoin, ainda falta capacidade transacional 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;

(v) 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;

(vi) Falta de regulação do próprio sistema: A falta de enquadramento legal e de suporte dos Estados pode representar um enorme risco para os utilizadores do sistema Bitcoin e, no limite, de outras manifestações da tecnologia Blockchain (todas têm um elemento de representação de valor monetário). Com efeito, e como vimos anteriormente, 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 índice NRI (já referido *supra*) 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.

No que tange a 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, consenso que pode versar as regras do sistema (*verbi gratia*, de determinação da validade de um bloco, o protocolo utilizado, ou o formato da informação), a história do sistema (particularmente, no que respeita ao histórico das transacções, registadas no Blockchain), e/ou consenso quanto ao facto de os *bitcoins* terem valor (Narayanan, 2016, 168-174).

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, devemos ter em consideração, 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.

Importa aqui considerar a posição que tem vindo a ser assumida pelo BCE, a respeito da tecnologia Bitcoin. No documento "Virtual currency schemes – a further analysis", o Bitcoin é integrado no conceito indefinido *esquemas de moeda virtual* (BCE, 2015, 4-5), juntamente com realidades tão distintas como por exemplo o Linden Dollar da plataforma Second Life (BCE, 2015, 6). Depois de identificar os aspectos negativos e os positivos do sistema Bitcoin, e de forma genérica referindo-se sempre aos VCS ("virtual currency schemes"), o BCE dá enfase ao facto de não existir um estatuto legal definido, e de haver o perigo de estarmos perante actividades não reguladas (BCE, 2015, 21). Depois, a análise prossegue para o que possa ser a perspectiva de um Banco Central relativamente a moedas virtuais, frisando-se aí que as moedas virtuais não são reconhecidas pelos Bancos Centrais do Eurossistema como dinheiro ou moeda, nem têm estatuto de moeda com curso legal (BCE, 2015, 23-25). Por fim, quando o BCE considera as respostas a adoptar pelos Estados europeus (a nível nacional), são identificadas as seguintes estratégias, todas, cremos nós, de reduzida ou nenhuma eficácia regulatória: alertar a sociedade para os riscos das moedas virtuais; licenciamento e supervisão de certos prestadores de serviços no âmbito das moedas virtuais; proibição de realização de transacções em moeda virtual.

Além disso, a falta de envolvimento de Bancos limita a protecção dos consumidores (*rectius*, dos utilizadores), nomeadamente, nos casos de furto dos *bitcoins*, perda das chaves de utilização (que redundam numa perda total do valor que representavam), entre outros casos.

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 abrangidos por estas regulações, sendo certo que é possível a utilização do sistema Bitcoin sem a intervenção de intermediários).

4. INCONSISTÊNCIAS DO BITCOIN

4.1. A descentralização do sistema Bitcoin

Do que temos vindo a investigar, é sugerido que a forma da rede Bitcoin, bem como as relações existentes entre os diversos intervenientes, assumem grande importância, contribuindo, nomeadamente, para a respectiva segurança. Aliás, é através da análise da rede e das relações aí estabelecidas que nos é possível caracterizar o sistema Bitcoin, e responder às nossas questões de investigação.

Conforme refere Assens (2014, 16), "Vista do ângulo da teoria das organizações, a rede é uma estrutura de colaboração, cujas convenções de trocas não dependem nem do mercado nem da hierarquia, Powell (1990) e Williamson (1991). A organização em rede é constituída por vários parceiros autónomos no plano financeiro, jurídico e/ou da gestão, mas mutuamente dependentes para atingir objectivos comuns."

Assens (2014, 19-20) refere que "o conceito de rede assenta em três princípios imutáveis – isto é, a autonomia, a interdependência, o afastamento – que afectam o comportamento dos membros e conferem modularidade à estrutura": (i) autonomia, na medida em que os membros da rede são autónomos entre si, são independentes; (ii) interdependência, no sentido de existir um desígnio comum entre os membros; (iii) afastamento, um princípio particularmente premente na rede Bitcoin, que é global e digital, mas que depende de uma difusão eficaz e célere da informação entre os seus membros.

Vimos que existem vários tipos de intervenientes na rede Bitcoin, sendo também diversas as funções que desempenham. Acresce que, sendo uma rede global, digital e codificada, a capacidade de análise da rede e das relações existentes (sejam de dependência ou outras) são de difícil concretização sem uma colaboração alargada dos próprios intervenientes (que podem não ter nenhum interesse em colaborar). Elucidativamente, Assens (2014, 22) entende que "Compreender o funcionamento destas redes consiste, então, em procurar, quase sempre, solidariedades invisíveis, fundadas no não dito e nas convenções." O que vem dificultar o trabalho de determinação do grau de centralização ou de descentralização que possa existir.

Partindo da análise de três dimensões (o pacto fundadora da rede, a sua arquitectura e as regras de relação) podem ser configurados três tipos de rede: "a rede distribuída, a rede pilotada, a rede administrada" (Assens, 2014, 55). Na rede distribuída os membros "ocupam posições simétricas e intermutáveis" significando isto que "nenhum membro exerce e uma função de pilotagem" (Assens, 2014, 56). Podemos falar aqui em autorregulação.

Já na rede pilotada "existe uma forma de hierarquia entre o membro colocado no cruzamento das comunicações, em posição de coordenador-geral, e os membros colocados na periferia", sendo atribuídas ao piloto, usualmente, "três competências específicas: a construção estratégica e a visão do futuro da rede (…); o estabelecimento e a consolidação de uma «atmosfera» de confiança (…); por último, a prospeção e a seleção dos novos parceiros." (Assens, 2014, 62-63).

Por fim, na rede administrada, "a colaboração entre os membros depende de regras institucionais: de uma carta de direitos e deveres no âmbito da adesão à rede. Uma estrutura de governança animada por membros eleitos é incumbida de fazer evoluir essas regras e de confirmar a sua aplicação junto dos membros aderentes." (Assens, 2014, 67).

Quadro 5: os diferentes tipos de governança da rede

	Rede distribuída *Modelo dominante nas redes sociais*	**Rede pilotada** *Modelo dominante na economia de mercado*	**Rede administrada** *Modelo dominante na economia social e solidária*
Pacto fundador	Solidariedade fundada nos valores comuns: o corporativismo, a lógica da honra e a reputação numa profissão, sentimento de pertença a um território, etc.	Solidariedade fundada nos ativos intangíveis (imagem de marca, tecnologia, competências) detidos pelo piloto	Solidariedade fundada na *affectio societatis*: a igualdade de tratamento com uma carta de direitos e deveres. Lógica de cooptação entre membros fundadores e novos membros
Arquitetura	Malha densa sem buraco estrutural. Posições dos membros intermutáveis e simétricas	Malha em forma de estrela/assimetria das posições. Poder central do piloto em posição de *broker*	Malha com substitutos de coordenadores de rede. Posição central da estrutura de governança agrupando os coordenadores de rede
Regra do jogo relacional	Governança pelas convenções/regulação pelos pares. Limite: os passageiros clandestinos	Governança encarnada pelo piloto/regulação contratual e jurídica. Limite: arbitrariedade do piloto	Governança por representantes «democráticos»/regulação política. Limites: peso da tecnoestrutura/conflito entre fundadores e não fundadores da rede

Fonte: Assens, 2014.

No Quadro 5 vemos, em detalhe, as três dimensões de análise de redes, e sua correspondência com os três tipos de rede. No caso da rede Bitcoin, não podemos dizer que exista uma correspondência perfeita a um dos três tipos de rede. Não obstante, a maioria da literatura refere-se à rede Bitcoin como uma rede descentralizada (que se aproxima da rede distribuída, por não ter um centro de decisão e de imputação de responsabilidades).

Para Narayanan *et al* (2017, 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?

Narayanan *et al* (2017, 27) 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, 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 sistema Bitcoin.

Para Beikverdi e Song (2015), os sistemas de pagamentos distribuídos (descentralizados) enfrentam vários problemas, que se podem agrupar em três categorias: (i) correcção (garantir a inexistência de transacções fraudulentas), (ii) concordância (entre os *nós* do sistema quanto a uma única verdade – o Blockchain é igual para todos) e (iii) 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): 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, 27-26) a noção de competição entre paradigmas de centralização e de descentralização é comum em diversas tecnologias digitais, reconhecendo que a descentralização não deve ser encarada como um "tudo ou nada", porque quase nenhum sistema é absolutamente descentralizado ou absolutamente centralizado.

Segundo Beikverdi e Song (2015), 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) 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, 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, tendencialmente centralizados.

Faggart (2015) 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".

4.1.2. Carteiras digitais:

Como vimos, 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, 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; Gervais *et al*, 2014, 4).

Estes intermediários funcionam sob lógicas de centralização, semelhantes às do sistema bancário. Ao centralizarem informação, tornam-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).

4.1.3. Mineração centralizada:

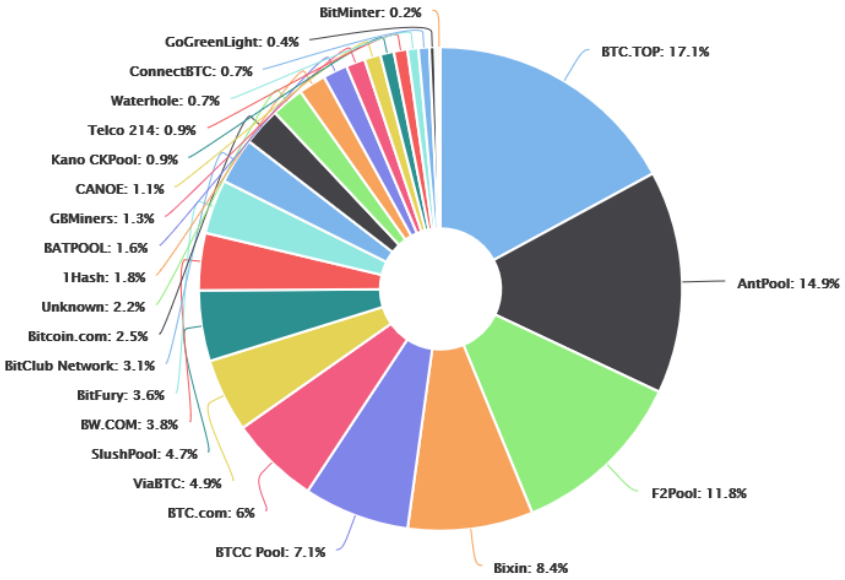
Por outro lado, a dificuldade dos puzzles matemáticos que os mineiros têm de resolver tem vindo a aumentar (o que decorre do aumento de capacidade computacional na rede). Em virtude desta dificuldade, e da ínfima probabilidade de um mineiro isolado conseguir o prémio pela resolução do puzzle (atribuição 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; Gervais *et al*, 2014, 3).

Neste contexto, 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), estes agrupamentos permitem reduzir a incerteza dos retornos (da lotaria) e garantir um rendimento regular (Gervais *et al*, 2014, 3).

Ademais, a entrada de novos intervenientes na rede Bitcoin (novos nós), tem justificado investimento em inovação de *hardware* e do *software* utilizado na mineração. Se no início era possível minerar *bitcoins* com um simples computador pessoal, actualmente, o processo de mineração só consegue ser realizado com eficácia mediante o recurso a *hardware/software* ASIC, ou seja, de forma profissional.

Beikverdi e Song (2015) consideram que 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, preferindo os novos intervenientes partilhar a sua força computacional num agrupamento de mineiros, tornando a rede Bitcoin cada vez mais centralizada. 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 transações de gasto duplo) (Gervais *et al* (2014, 3). 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)



Fonte: https://blockchain.info/pt/pools

(consultado em Junho de 2017)

Este gráfico é elucidativo da capacidade computacional de algumas Pools de Mineiros. O momento retratado pelo Gráfico 10 (a capacidade computacional não é estável, oscilando a cada instante) demonstra que juntando apenas 4 Pools fica reunida a maioria da capacidade computacional da rede. No passado já se registou, em inúmeras ocasiões, uma Pool ter mais do que 50% da capacidade computacional.

Acresce a este enquadramento, o facto de serem desconhecidas as relações entre Pools de Mineiros, sendo certo que um mesmo grupo económico pode estar por trás de várias Pools, diluindo dessa forma a aparência de domínio absoluto e de captura do sistema.

Como temos vindo a referir, o próprio criador do sistema Bitcoin sustenta que a segurança depende de nenhum mineiro possuir mais de 50% da capacidade computacional (e de voto).

4.1.4. Actualizações do protocolo Bitcoin:

Segundo Gervais *et al* (2014, 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) 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, 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, 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, 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, 6), o facto de o poder estar concentrado pode facilitar a pressão dos Estados e das entidades reguladoras.

4.1.5. Centralização do mercado de transacções:

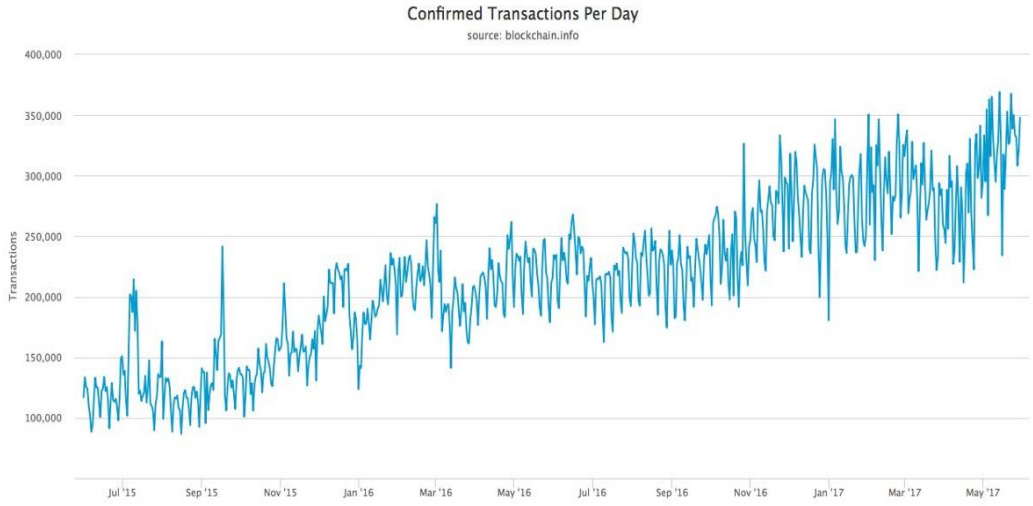
Shin (2017) põe em evidência que o sistema Bitcoin não tem conseguido resolver o problema do aumento do volume de transacções perante uma rede cuja capacidade estagnou, levando a um aumento de comissões cobradas por transacção. Este facto, segundo Garzik (*apud* Shin, 2017) "empurra" os utilizadores para intermediários virtuais (centralizados).

Por outro lado, Shin (2017) sublinha também a incapacidade da rede perante o avolumar de transacções que se traduz em demoras no registo de muitas transacções. Em sentido concordante, Baxter (2017) faz uma analogia entre os mineiros e as portagens da autoestrada, sustentando que ambos funcionam da mesma forma: os mineiros preferem que exista muito tráfego pois isso aumenta os seus ganhos (*transaction fees*). 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)

Resulta dos Gráficos 11 e 12 que as comissões pagas por transacção aos mineiros tem crescido de forma mais rápida do que o número de transacções, o que pode indiciar, de facto, uma sobrecarga da rede, como refere Shin (2017).

4.1.2. Impactos da centralização

4.1.2.1. Segurança do sistema:

Nakamoto (2008, 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 *51% Attack*, mediante o qual consegue subverter as regras do sistema, manipulando as transações (Beikverdi e Song, 2015). Shin (2017) refere que os ataques de rede podem ser de três tipos: violação da confidencialidade (divulgação da identidade dos intervenientes nas transacções), da disponibilidade (limitação e/ou interdição do acesso à rede) ou da integridade (alteração/adulteração das próprias transacções).

Courtois e Bahack (2014) 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; Shin, 2017). Para Courtois e Bahack (2014), "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."

Beikverdi e Song (2015) 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 uma condição da segurança.

4.1.2.2. A confiança e o Bitcoin:

Para Nakamoto (2008, 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, 6).

Dodd (2017, 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) 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, é tão vulnerável 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*), o que pode ser ruinoso para a reputação do Bitcoin (Faggart, 2015).

4.2. A função de pagamentos (meio de troca)

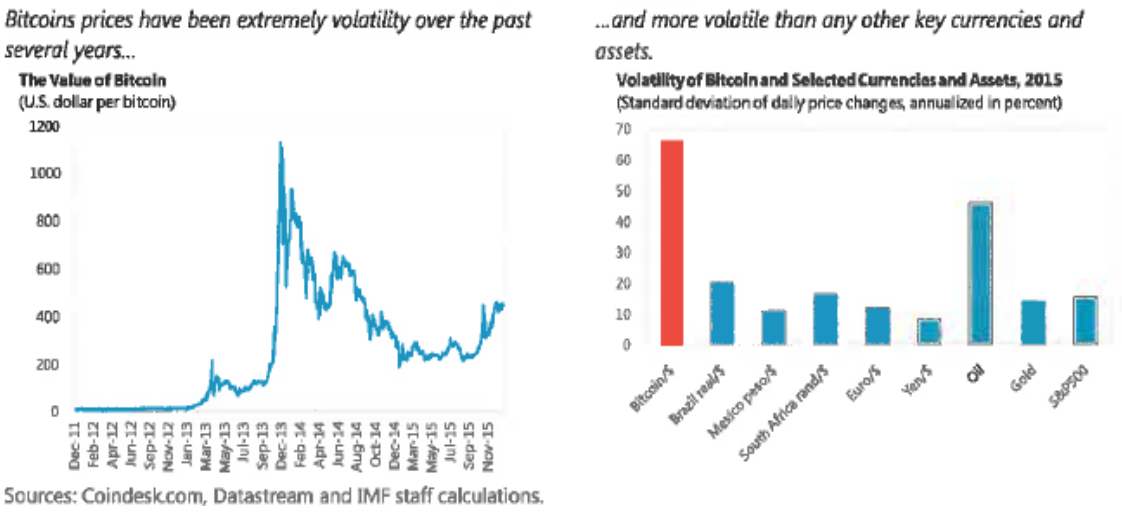
Como vimos *supra* no Capítulo II, a moeda desempenha três funções: meio de troca, unidade de conta e instrumento de reserva de valor. De acordo com Guadamuz e Marsden (2014, 4), as moedas foram inventadas com o objectivo de facilitar a troca, para facilitar as transacções. No Capítulo III vimos que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

4.2.1. A volatilidade

Estas características resultam, segundo Guadamuz e Marsden (2014, 6), da própria arquitectura do protocolo Bitcoin, que integra a escassez como uma condição, limitando a oferta monetária. Para Antonopoulos (2014, 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 unidades monetárias no mercado.

Uma das consequências decorrentes da arquitectura monetária do sistema Bitcoin é a volatilidade da respectiva unidade monetária. Vimos nos Gráficos 8 e 9 (páginas 45 e 46, respectivamente, a valorização da unidade monetária *bitcoin*.

Gráfico 13 e 14: valorização dos bitcoins e respectiva volatilidade, por comparação com outras moedas e matérias-primas



Fonte: Virtual currencies and beyond (IMF, 2016).

Resulta destes gráficos, particularmente do Gráfico 11, que nenhuma outra moeda ou matéria-prima regista um nível tão elevado de volatilidade. Se associarmos esta volatilidade à oferta monetária limitada, resulta daqui um enorme incentivo à não utilização dos *bitcoins*.

4.2.2. *bitcoin hoarding*

Neste sentido, Antonopoulos (2014, 176) sublinha que esta natureza deflacionária tem promovido a retenção dos *bitcoins* (*bitcoin hoarding*), que assumem, assim, uma dimensão mais acentuada de instrumento financeiro.

Guadamuz e Marsden (2014, 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 adereço para outro."

Hanley (2015, 9) concorda com esta posição, reafirmando que nenhum agente económico racional utilizaria os Bitcoins, em valorização permanente, 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.

No entanto, Antonopoulos (2014, 176) considera que este "instinto de retenção" pode ser ultrapassado se o mercado promover a utilização dos Bitcoins, enquanto meio de pagamento, mediante incentivos económicos adequados.

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 instrumento financeiro alternativo aos modelos de negócios clássicos do sistema financeiro. Desde logo, pela eficiência e pela redução dos custos associados às transações.

5.1. Respostas à pergunta de partida e às questões de investigação

Começamos por sugerir que o sistema Bicoin, ao contrário do que é usualmente anunciado, tende a ser centralizado em muitos aspetos (mineiros, *developers*, *wallets*), facto que pode promover a falta de credibilidade do sistema e à potencial descrença dos utilizadores.

Assim, respondemos negativamente à nossa segunda questão de investigação (Q2) **O sistema Bitcoin é descentralizado?**

Ademais, a natureza tendencialmente deflacionária inerente do sistema Bitcoin, assente numa oferta monetária fixa e predeterminada, dificulta a sua consideração como moeda, uma vez que os utilizadores tenderão a não utilizar os seus *bitcoins*. Este facto potencia a utilização do sistema Bitcoin pelos especuladores, com vista a ganhos futuros.

Contudo Rogoff (2017, 281) sugere que “as pessoas deviam de se preocupar muito mais com a inflação do que com a deflação. Porquê? Porque o bitcoin não tem o monopólio sobre a tecnologia em que se apoia, e podem aparecer imitadores” como na verdade, já existem. Em regra, os "seguidores” conseguem vantagens comparativas perante os inovadores.

Neste enquadramento, Rogoff (2017, 281) questiona “será que o estado pode, de facto, copiar estas novas tecnologias para criar um mecanismo de compensação superior para a sua moeda eletrónica?” concluindo “se chegar a haver uma moeda digital supervisionada pelo Estado – por exemplo, uma *bencoin* -, o seu impacto no sistema financeiro poderá ser bastante dramático,

afetando significativamente a capacidade de os bancos privados de se envolverem na transformação de liquidez".

(Q3) **Os *bitcoins* são utilizados (maioritariamente) como meio de pagamento ou como instrumento financeiro?**

Desta forma, e em resposta à nossa terceira questão de investigação resulta da análise que a maioria dos *bitcoins* não regista qualquer movimento, sendo que o trabalho de campo sugere que os mesmos tender a estar "guardados" pelos seus proprietários, pelo que podemos considerar que a sua utilização preferencial é como instrumento financeiro de pendor especulativo.

Nesta análise vale recordar Turner (2016, 330), quando refere que "é necessário uma nova abordagem da economia e da política pública. A ortodoxia anterior à crise refletiu um excesso de confiança no poder dos mercados financeiros livres para obterem resultados ótimos" sendo que a abordagem futura "tem de reconhecer que tanto os mercados como os governos podem falhar e que a política ótima envolve, inevitavelmente, uma escolha entre imperfeições alternativas e perigos alternativos."

Chegados à análise da "pergunta de partida"

(Q1) O modo de funcionamento (a prática) do sistema Bitcoin tende a traduzir o objectivo (a ideia) da sua criação?

Podemos observar que, apesar da notoriedade crescente do sistema Bitcoin, consideramos, depois de revista a literatura existente, que a realidade deste sistema tende a não corresponder às ambições tangíveis do seu arquiteto.

No entanto ainda é cedo para se fazer história.

Trata-se de um projeto novo, e disruptivo. E motivador de pistas e de atuações para os diversos *players*.

Foram identificados "espaços vazios" nos modelos de negócios do clássico sistema financeiro. Para Oliveira (2017, 59), "é neste contexto que se tem afirmado que os bancos passam por um "ciclo de sofrimento" (um *grief cycle*) composto por cinco estados de infelicidade e adaptação à nova realidade da tecnologia financeira", podendo observar-se um novo despertar.

Investigamos e dissertamos sobre dois modelos complementares (o modelo financeiro vigente e o do Bitcoin), e acreditamos que a capacidade de criar sinergias e parcerias entre ambos poderá oferecer cenários de sucesso. Evocando Henry Ford, e as suas expressivas palavras quanto ao

valor das parcerias… “Coming together is a beginning. Keeping together is progress. Working together is success.”

O modelo de colaboração, como sempre, vai ajustar-se ao longo do tempo. Sempre assim o foi.

5.2. Pistas de investigação futura

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.

6. 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 nº. 5, 2014, pp. 462-482, DOI 10.1108/FS-06-2013-0024.

Assens, Christophe (2014), *A gestão das redes – Tecer laços sociais para o bem-estar económico*. Lisboa: Edições Piaget.

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.

Bower, Joseph, e Christensen, Clayton (1995), Disruptive technologies: Catching the wave, *Harvard Business Review*, Janeiro-Fevereiro 1995.

Brito, Jerry e Castillo, Andrea (2016), *Bitcoin: A primer for policemakers*, 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.

Champagne, Phil (2014). *The book of Satoshi: The collected writtigs of bitcoin creator Satoshi Nakamoto*, USA: e53 Publishing.

Coase, Ronald (1937). The nature of the firm, *Economica*, New Series, Volume 4, Número 16, Novembro, 1937, pp. 386-405, Reino Unido.

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 observer e interpreter 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 xeque-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.

Oliveira, Ana Perestrelo (2017). The nature of the firm, *Economica*, New Series, Volume 4, Número 16, (Nov., 1937), pp. 386-405, Reino Unido

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 paradigma of global information society, *Ekonomické Rozhl'Ady – Economic Review*, Volume 45, N.º 3, p. 295-311.

Turner, Adair (2015) *Between debt and the devil: Money, credit, and fixing global finance*, Nova Jersey (USA): Princeton University Press.

Ulrich, Fernando (2014), *Bitcoin – A moeda na era digital*", São Paulo (Brasil): Instituto Luwig 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.

Williamson, Oliver (1975, 1983). *Markets and hierarchies - Analysis and antitrust implications: a study in the economics of internal organization*. Nova Iorque (USA): Free Press.

7. WEBGRAFIA

Baxter, Christian (2017), *The Bitcoin Game Theory*. Disponível em: https://medium.com/@cbaxter/the-bitcoin-game-theory-878b6f479a0b

Banco Central Europeu (2015), *Virtual currency schemes – A further analysis*. Disponível em: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf

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*, *Criptography 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