GUIA JURÍDICO PARA A TECNOLOGIA BLOCKCHAIN

TIAGO DA CUNHA PEREIRA

REVISTA DE DIREITO FINANCEIRO E DOS MERCADOS DE CAPITAIS, VOL. 1 (2019), NO. 4, 355-400

TIAGO DA CUNHA PEREIRA
Advogado-estagiário, Mestre em Direito e Gestão

Guia Jurídico para a tecnologia *Blockchain*[1]

A Legal Guide to Blockchain technology

Resumo: O presente estudo procura transmitir um entendimento panorâmico das principais problemáticas em torno das tecnologias blockchain, com especial enfoque nas potencialidades e desafios apresentados.

Palavras-chave: (i) bitcoin; (ii) blockchain; (iii) initial coin offerings; (iv) peer-to-peer arbitration; (v) smart contracts.

Abstract: The present study aims to establish a panoramic understanding of the main legal matters surrounding blockchain technologies, with special focus on the opportunities and challenges they present.

Keywords: (i) bitcoin; (ii) blockchain; (iii) initial coin offerings; (iv) peer-to-peer arbitration; (v) smart contracts.

Sumário: I – Introdução às tecnologias *Blockchain*: 1. *Timestamping*; 2. Autenticação em rede; 3. Incentivo; 4. Privacidade. II – *Legal Tech e Blockchain*: 1. Criptoativos; 2. *Smart Contracts*: 2.1. *Peer-to-peer arbitration*; 2.2. Serviços financeiros; 2.3. Economia colaborativa; 2.4. O caso particular da distribuição de energia; 3. *Initial Coin Offerings* ("ICOs"): 3.1. Conceito e estrutura; 3.2 ICO vs. IPO; 3.3 Vantagens das ICOs. III – Desafios de implementação: 1. Desafios

[1] O estudo que se segue é baseado na dissertação para a obtenção do título de Mestre em Direito e Gestão, apresentada à Universidade Católica Portuguesa – Centro Regional do Porto, sob o título "Aplicações Jurídicas das Tecnologias Blockchain".

operacionais: 1.1 Capacidade de processamento; 1.2 Dimensão; 1.3. Insustentabilidade; 1.4 Iliteracia informática; 2. Desafios legais e regulatórios: 2.1. Incerteza legal e regulatória; 2.2. (In)Segurança; 2.3. Utilização indevida

I – INTRODUÇÃO ÀS TECNOLOGIAS *BLOCKCHAIN*

As tecnologias *blockchain* (doravante, apenas "*blockchain*") nasceram a 31 de outubro de 2008 com a publicação do artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*" por Satoshi Nakamoto – autor desconhecido à data de hoje. Insatisfeito com o sistema financeiro tradicional, mormente com a sua dependência de intermediários prestadores de "serviços de confiança"[2]-[3], Nakamoto pretendia criar uma versão eletrónica de dinheiro que não dependesse de um operador central e estivesse livre do controlo de qualquer Governo ou Banco Central[4].

A proposta de solução passava por substituir a necessidade de confiança, inexoravelmente ligada a custos de intermediação por uma terceira parte, por provas criptográficas, automatizadas, sem possibilidade de interferência por qualquer sujeito. Ao invés de se encontrar no servidor de uma entidade gestora, a base de dados é

[2] *Vide* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, acessível em: https://bitcoin.org/bitcoin.pdf (consultado a 18 de outubro de 2019), 1.

[3] Atualmente, podemos encontrar as definições de "serviço de confiança" e "prestador de serviço de confiança", respetivamente, nos n.os 16 e 19 do artigo 3.º do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014 relativo à identificação eletrónica e aos serviços de confiança para as operações eletrónicas no mercado interno.

[4] A aversão ao controlo por uma entidade central relaciona-se com o desejo de anonimato e de prevenção do problema do "Duplo Gasto", um dos maiores obstáculos que a conceção de dinheiro virtual enfrenta desde os seus primórdios. O dinheiro virtual não mais é do que uma sequência alfanumérica, pelo que facilmente se entende que a sua transferência não implica necessariamente a entrega da moeda com curso legal a ele associada. Ora, se um utilizador copiar esse código e posteriormente o transferir a dois comerciantes diferentes, é certo que pelo menos um deles não vai receber a moeda (ou o direito a esta) associada à sequência fornecida pelo utilizador. Hoje, evitamos os problemas de Duplo Gasto com recurso aos "serviços de confiança" supramencionados – os *VISA*, *Mastercard*, *Paypal*, *Western Union*, Bancos, e afins -, os prestadores de serviços de pagamento.

pública, podendo cada utilizador descarregar a *blockchain* de Nakamoto para o seu computador. As operações são aprovadas por todos os nódulos ("*nodes*"[5]) que integram o sistema. Os grupos de operações são agrupados num bloco ("*block*") que tem o seu lugar específico numa cadeia ("*chain*"), onde antecede e é precedido de outras operações. A cada dez minutos, todos os nódulos comunicam entre si e atualizam as respetivas bases de dados com as operações que, entretanto, ocorreram. A segurança da informação fica assegurada por esta descentralização; se um indivíduo alterar o conteúdo de um ou mais blocos registados na cadeia, assim que o seu nódulo comunicar com a rede, a sua cadeia de operações será tida como errada, rejeitada pela rede, e automaticamente corrigida. Deste modo, fica também assegurada a irrevogabilidade das operações, uma vez que o único meio de alterar o conteúdo de blocos passados é conseguir que, pelo menos, 51% dos nódulos da rede o façam também (e em igual medida).

O sistema proposto resume-se (embora simplisticamente, por forma a não exceder objeto do nosso labor) a quatro pilares: **(i)** *timestamping* ("carimbo de tempo"); **(ii)** autenticação pela rede; **(iii)** incentivo, **(iv)** e privacidade.[6-7-8]

1. *Timestamping*

A *blockchain* carimba grupos de operações, publicando para toda a rede, em seguida, o *hash code* correspondente ao bloco em questão. O *hash code* não mais é do que um carimbo que atesta que

[5] Nome cunhado por Nakamoto para apelidar todos os pontos de acesso (por norma, computadores ou telemóveis) à sua *blockchain*.

[6] *Vide* Satoshi Nakamoto, ob. cit., 2-6.

[7] O número de pilares varia consoante os autores. Embora todos destaquem as mesmas características, alguns escolhem autonomizar ideias que, para manter esta introdução sintética, escolhemos agregar. Neste sentido, referindo sete princípios, Don Tapscott/Alex Tapscott, *Blockchain Revolution*, 2ª edição, Portfolio Penguin, 2018, 29-52.

[8] Referindo sete pilares, embora diferentes, Aaron Wright/Primavera De Filippi, *Blockchain and the Law: the rule of code*, Harvard University Press, 2018, 33-45.

a informação em causa existiu no período temporal registado na rede. Cada bloco contém o *hash code* do bloco anterior, solidificando a informação[9]. Se um bloco for alterado por decisão de 51% da rede, o seu *hash code* vai obrigatoriamente mudar também. Como cada bloco contém o código do bloco que o antecede, para alterar um bloco da cadeia, será necessário alterar também todos os que se seguem. Consequentemente, o *timestamping* assegura tanto a rastreabilidade de toda a informação contida na rede, como a solidez da informação nela inserida[10].

2. Autenticação pela rede

Quando duas partes comunicam à rede a intenção de contratar, torna-se necessário que esta autentique a operação. Tal é feito através do método *Proof-of-Work*. A rede difunde todos os novos pedidos de operação para os nódulos que a integram. Cada nódulo recolhe um grupo de pedidos de operação, contido num bloco. Para cada bloco, a rede cria uma espécie de puzzle matemático e comunica-o a todos os computadores, para que o procurem resolver - este método exige um nível considerável de poder computacional[11]. A chave do "puzzle"[12] é aleatoriamente gerada pela rede, para que todos os com-

[9] *Vide* Satoshi Nakamoto, ob. cit., 2.

[10] Paralelamente, é possível alterar todas as operações efetuadas numa determinada rede após um certo ponto, desde que 51% da mesma vote nesse sentido. Este fenómeno é frequentemente utilizado por grupos que pretendem alterar o modo de funcionamento de uma *blockchain*. Quando bem-sucedido, o grupo maioritário cria uma nova *blockchain*, em tudo semelhante à anterior, com exceção da regra ou regras para cuja mudança estes votaram, agora alteradas em conformidade. Este fenómeno é apelidado de "fork" ("bifurcação"), dado o facto de um conjunto de utilizadores ter decidido seguir um caminho diverso dos restantes.

[11] Neste subcapítulo, referimo-nos especificamente a "computadores", porque, tendo em conta o poder computacional exigido para a validação de operações, os telemóveis não são ainda um instrumento viável para este tipo de operação.

[12] Apelidada de "*nonce*", expressão inglesa sem tradução direta, que significa algo utilizado apenas uma vez ou desenhado para uma ocasião só.

putadores tenham igual chance de chegar à resposta[13]. Como não existe *know-how* envolvido na equação, os computadores procuram a solução numa base de tentativa e erro. Sempre que produzirem um código (leia-se "resposta") que não coincide com o que a *blockchain* formulou, este é rejeitado e o computador reinicia o processo de formulação[14].

A ideia assenta num princípio de igualdade, mas não é perfeita. Como a eletricidade, espaço vago no disco rígido e poderio do processador são os fatores envolvidos, um computador topo de gama conseguirá produzir mais respostas no mesmo período temporal que um computador menos eficiente, tendo, teoricamente, mais probabilidades de acertar a chave que valida a operação.

Uma vez encontrada a resposta, o computador responsável transmite a mensagem para todos os nódulos da rede. Os nódulos aceitam este novo bloco se todas as operações nele contidas forem válidas. Por exemplo, se nos comprometemos a comprar um livro por dez criptomoedas e apenas temos cinco em carteira, a operação é rejeitada pela rede, pese embora o nódulo tenha chegado à resposta correta para validar o bloco, eliminando o risco de Gasto Duplo.

A aceitação por parte da rede, que mais não é do que a soma dos nódulos que a compõem – relembre-se que inexiste uma autoridade central –, é feita quando estes começam a validação do bloco de operações seguinte, reconhecendo o *hash code* de um bloco como sendo o anterior ao da operação a validar agora.

3. Incentivo

Para que os nódulos da rede queiram despender do seu poder computacional, eletricidade e tempo na validação de operações de terceiros, é oferecido um criptoativo ao primeiro a encontrar a solu-

[13] Isto é importante para o incentivo dos nódulos, como adiante falaremos.

[14] Assim se compreende a nomenclatura adotada, uma vez que cada resposta surge como uma prova do trabalho ("*Proof-of-Work*"), e não como uma qualquer produção de intelecto ou qualidade superior às dos seus pares.

ção ao puzzle gerado pela *blockchain*. Assim se assegura a distribuição inicial das criptomoedas[15] criadas por Nakamoto[16].

As partes acordam ainda uma taxa de operação a pagar aos nódulos, por forma a assegurar o incentivo à validação após a distribuição inicial de todas as criptomoedas.[17] O valor da taxa é voluntariamente decidido, mas os nódulos não são obrigados a aceitar qualquer operação. Naturalmente, as operações com taxas mais elevadas levarão ao concurso de vários nódulos, resultando numa aprovação mais célere. Este mecanismo é ainda importante para a prevenção de mensagens de *spam* ou outros conteúdos indesejáveis, uma vez que o seu autor terá de pagar à rede para os difundir, tornando-os, em grande parte, inviáveis.

Por fim, este pagamento aos nódulos desempenha uma importante função de incentivo à honestidade. Supondo um cenário em que um utilizador consegue angariar 51% do poder computacional numa rede, obtendo a prerrogativa de unilateralmente reverter as operações nela realizadas, o incentivo financeiro para validar novas operações será sempre superior ao de reverter as anteriores. A ideia subjacente consiste em tornar as fraudes mais custosas do que os seus possíveis benefícios. É neste sentido que Don e Alex Tapscott dizem que o sistema alinha os interesses de todos os seus *stakeholders*[18].

4. Privacidade

Cada utilizador tem uma chave privada para aceder à rede e uma chave pública para nela se identificar a outros utilizadores.

[15] Existem outros tipos de criptoativos, mas a *blockchain* de Nakamoto funciona em torno de uma criptomoeda. A seu tempo, faremos a devida distinção.

[16] O processo contínuo da procura de códigos que validem operações na rede, conforme definido em **2.**, com vista à obtenção de recompensa sob a forma de criptomoedas, é comumente denominado de "mineração".

[17] A *blockchain* de Nakamoto tem um número finito de vinte e um milhões de criptomoedas, cada uma divisível até à oitava casa decimal.

[18] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 35.

Ambas as chaves não passam de um conjunto alfanumérico de carateres; inexistem endereços de correio eletrónico, números de telemóvel ou quaisquer outros dados pessoais dos utilizadores.

No entanto, todas as operações são públicas. Qualquer utilizador pode ver o histórico de operações de uma chave pública na rede, embora não saiba a que pessoa aquela chave corresponde. A ideia foi, parece-nos, contornar a hegemonia de informação a que os intermediários de crédito e prestadores de serviços de pagamento usualmente têm acesso. Não obstante, este é, para nós, um dos aspetos criticáveis da *blockchain* de Nakamoto, conforme trataremos de expor no capítulo III.

O que é então uma *blockchain*? Atrevemo-nos a definir o conceito como uma base de dados, desenhada para ser distribuída por vários utilizadores, ser imutável (ou dificilmente reversível), funcionar sem o controlo de nenhuma entidade central e dispensar a necessidade de os utilizadores confiarem uns nos outros.

A *Bitcoin*, criada por Nakamoto e ainda hoje a mais utilizada, é uma *blockchain* pública, sem qualquer permissão de acesso ou controlo sobre as operações efetuadas. Outras existem onde, pese embora o acesso seja público, há a necessidade de controlar um ou mais funcionalidades. São chamadas de *blockchains* híbridas[19]. Por fim, existem várias blockchains privadas, onde o acesso está sujeito à permissão da entidade criadora e o consenso é por ela estabelecido[20] [21].

A *Bitcoin* foi de facto a primeira e é ainda hoje a mais mediática das *blockchains*. Na sua essência, é dinheiro eletrónico, chamado

[19] Por exemplo, *Bigchain DB*; *Evernym;* e *Alastria*.

[20] A título de exemplo, o *Santander* gere uma blockchain privada, restrita a um grupo de trabalhadores ou clientes, a Santander One Pay FX.

[21] As tecnologias *blockchain* são uma forma de tecnologia de contabilidade distribuída ("*distributed ledger technologies*", doravante "DLTs"). O termo DLT apresenta-se como mais amplo face a *blockchain*, englobando todos os tipos de *blockchains* existentes. Todas as DLTs operam num modelo descentralizado e baseado em criptografia, semelhante ao que exporemos neste capítulo; no entanto, as restantes caraterísticas – máxime o acesso e governo da rede – variam consoante o tipo de tecnologia em causa, existindo por isso, e como veremos, essencialmente três tipos de *blockchains*.

hoje de "criptomoeda", com os objetivos que o seu criador projetou. Mas, se há uma ideia que queremos que o leitor leve deste capítulo, é que a *blockchain* não é a *Bitcoin*. Baseamo-nos nos princípios de Nakamoto para explicar as funcionalidades desta tecnologia de contabilidade distribuída, porque os seus princípios estão, em maior ou menor medida, assentes nas *blockchains* que se seguiram. Hoje, estas tecnologias vão muito além da *Bitcoin* e das restantes criptomoedas[22]. É comum falar-se da *Bitcoin* como "*Blockchain 1.0"* e das aplicações subsequentes como *"Blockchain 2.0"*[23].

Este trabalho não versa sobre uma rede ou um grupo de redes. A nossa ideia, de ora em diante, é trazer à colação algumas das potencialidades com que esta tecnologia tem seduzido o mundo jurídico, apresentadas por diversas *blockchains* de tipos variados.

II – *LEGAL TECH* E *BLOCKCHAIN*

Abreviatura de "*Legal Technology*", a *legal tech* resume-se à afetação de tecnologia à prática jurídica. Ao contrário das *blockchains*, a *legal tech*, já existe há vários anos, com exemplos bastantes na prática judiciária portuguesa[24]. São também conhecidas inúmeras plataformas que recolhem, organizam e divulgam, na sua página ou com base em serviços de subscrição, novidades legislativas, jurisprudenciais, artigos de relevo e notícias de destaque para o mundo jurídico. Também estas são *legal tech*.

Entre nós, existe quem adote o termo "Tecnologia Descentralizada de Registo de Dados". Cfr. Francisco Mendes Correia, *A tecnologia descentralizada de registo de dados (Blockchain) no sector financeiro*, em "Fintech: Desafios da Tecnologia Financeira", Almedina, 2019.

[22] Para referência futura, sempre que nos referirmos a "criptoativo", estamos a empregar um tema que engloba tanto "*coins*" – criptomoedas, uma unidade de valor dentro de uma *blockchain* – como "*tokens*" – um bem que, para além de unidade de valor, tem subjacente um ativo ou direito.

[23] Também por esta nomenclatura se entende a importância da primeira criptomoeda no fomento tecnológico das DLTs.

[24] A plataforma *Citius*, onde advogados, solicitadores, juízes e magistrados podem gerir os seus processos judiciais, é um exemplo de legal tech. A assinatura digital dos advogados é também uma manifestação da tecnologia aplicada ao mundo jurídico.

Quanto aos objetivos, a *legal tech* pode ser dividida em oito categorias[25], mas apenas duas relevam para o escopo do nosso labor: automatização documental e proteção de dados.

A primeira, como o próprio nome indica, assenta na construção de um sistema que, com base em segmentos de texto e/ou dados pré-existentes, seja capaz de construir um novo documento. Imagine-se um contrato de arrendamento onde as partes podem escolher de entre um leque de cláusulas previamente elaboradas e inseridas num sistema. O contrato equivalerá à soma de todas as disposições que as partes acordem incluir.

As tecnologias de proteção de dados, ao contrário do que o seu nome sonante possa fazer parecer, têm já um longo histórico, datando muito antes do atualmente famoso Regulamento Geral de Proteção de Dados[26]. O exemplo mais usual é talvez o uso do software *WinRAR* para enviar ficheiros, encriptados com uma palavra-passe à nossa escolha, a terceiros.

A relevância para o nosso ensaio vem, não da eclosão deste tipo de tecnologias, mas das potencialidades do uso de *blockchains* enquanto *legal tech*[27]. Em seguida, expomos aquelas que, na nossa opinião, configuram algumas das oportunidades mais proeminentes, cientes de que as mesmas devem ser lidas em conjunto com os desafios levantados no capítulo III[28-29-30].

[25] Quanto às oito categorias de *Legal Tech*, *vide* Sabrina Praduroux/Valeria De Paiva/Luigi Di Caro, *Legal Tech Start-ups: State of the Art and Trends*, Universidade de Turim, 2016, acessível em: https://vcvpaiva.github.io/includes/pubs/2016-legal.pdf (consultado a 18 de outubro de 2019), 2-4.

[26] Referimo-nos ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[27] Chegando mesmo a existir quem fale de um novo ramo de direito, a "*Lex Cryptographia*". Neste sentido, *vide* Aaron Wright/Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, acessível em: http://ssrn.com/abstract=2580664 (consultado a 18 de outubro de 2019), 4.

[28] Aos quais acresce a conceção generalizada de que o mínimo avanço tecnológico pode destabilizar gravemente um sistema jurídico e a baixa literacia tecnológica dos profissionais juristas. Neste sentido, *vide* AA.VV., *Legal Technology Vision*, Signapore Academy of Law, 2017, acessível em: https://www.sal.org.sg/Resources-Tools/Legal-Technology-Vision (consultado a 18 de outubro de 2019), 4-6.

1. Criptoativos

O facto de o nosso tema ter surgido de uma criptomoeda justifica que os criptoativos, pese embora não sejam hoje, na nossa opinião, o principal incremento das DLTs no mundo jurídico, sejam o primeiro ponto do presente capítulo.

Como o próprio nome indica, os criptoativos extravasam o domínio das criptomoedas. Estas últimas, sucintamente descritas no capítulo introdutório, constituem essencialmente um meio de pagamento eletrónico[31]. Face às moedas metálicas e notas[32], as criptomoedas apresentam uma clara vantagem - não necessitam de armazenamento. Face à moeda escritural, oferecem um prazo de compensação muito inferior para a generalidade das operações.

[29] Em sentido oposto à nota de rodapé anterior, e no que toca à advocacia em específico, *vide* McGinnis e Pearce defendem que a automatização de documentos não é completamente viável, por existirem ramos jurídicos, como o direito bancário e o dos valores mobiliários sujeitos a mudanças legais e regulatórias em curtos espaços de tempo. *Vide John O.* McGinnis/Russel G. Pearce, *The great disruption: how machine intelligence will transform the role of lawyers in the delivery of legal services,* Fordham Law Review n.º 82, 2014, acessível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5007&context=flr (consultado a 18 de outubro de 2019), 3042.

[30] "*The question is thus not whether to "allow" AI based software and digital innovation to enter into legal space, but rather how to determine the rights and duties of the stakeholders on the new type of playground.*", *vide* Tanel Kerikmäe/Thomas Hoffmann/Archill Chochia, *Legal Technology for Law Firms: Determining Roadmaps for Innovation,* Croatian International Relations Review, Vol. 24, n.º 81, 2018, acessível em: https://hrcak.srce.hr/199994 (consultado a 18 de outubro de 2019), 100.

[31] Poderíamos ainda equacionar a capacidade da *Bitcoin* para desempenhar uma função de reserva de valor, mas tal não é hoje possível devido à extrema volatilidade associada à criptomoeda. Adiante trataremos este tema.

[32] Os Estados Membros podem emitir moedas correntes, comemorativas e de coleção, estando os respetivos volumes de emissão sujeitos a aprovação do Banco Central Europeu. Todas as moedas correntes e comemorativas expressas em euros têm curso legal e poder liberatório nos termos definidos no art. 128.º n.º 2 do Tratado sobre o Funcionamento da União Europeia e no art. 11.º do Regulamento (CE) n.º 974/98.
Compete exclusivamente ao Banco Central Europeu emitir ou autorizar a emissão de notas na União Europeia. Tal resulta do art. 128.º n.º 1 do Tratado sobre o Funcionamento da União Europeia.

A generalidade da população, avessa ao risco, confia a guarda do seu dinheiro a instituições financeiras, que o agradecem, por verem nele uma forma de aforro para a sua atividade.

Tradicionalmente, este contrato era simbiótico: o depositante confiava o seu dinheiro ao depositário, financiando a sua atividade, e este segundo remunerava a confiança do primeiro mediante o pagamento anual de um juro sobre o valor depositado.

No entanto, no pós-crise financeira de 2008, a confiança dos investidores foi abalada. A ideia de uma instituição financeira *too big to fail* foi desmistificada e, compreensivelmente, os aforradores não se sentiram confortáveis em arriscar capital. A este cenário foi adicionada uma garantia do capital depositado[33], estabelecendo-se um clima de inércia dos investidores na União Europeia.

A conjuntura descrita firmou na população a ideia do depósito à ordem como o único produto bancário isento de risco, pelo que o mesmo notou um engrandecimento generalizado. Perante a afluência dos depósitos à ordem, os bancos viram-se forçados a depositar o seu excesso de liquidez junto do Banco Central Europeu (doravante, "BCE"). Em alternativa, apenas poderiam equacionar conceder mútuos a outros bancos; no entanto, o excesso de liquidez era um problema de tal modo generalizado que nenhuma instituição de crédito tinha interesse em contrair obrigações (pelo contrário), por muito atrativas que as taxas de juro pudessem ser. Uma outra opção seria o investimento em ativos, comportando um nível de risco superior, nível esse que nem as instituições de crédito nem os particulares se sentiam confortáveis em assumir, especialmente em Portugal.

Devido ao excesso de oferta e falta de procura, em 2014, o BCE aplicou pela primeira vez uma taxa de juro negativa às reservas de

[33] O Fundo de Garantia de Depósitos encontra-se regulado nos artigos 154.º e ss. do Regime Geral das Instituições de Crédito e Sociedade Financeiras. Por norma, garante o reembolso, por instituição de crédito, do valor global dos saldos em dinheiro de cada titular de depósito, até ao limite de 100.000 €, conforme definido no art. 166.º do mesmo diploma. O Fundo de Garantia do Crédito Agrícola Mútuo, regulado pelo Decreto-Lei 345/98, de 9 de novembro, desempenha uma função equivalente para a Caixa Central de Crédito Agrícola Mútuo e para as caixas de crédito agrícola mútuo suas associadas.

bancos europeus nele depositadas[34] [35], isto é, cobrou para receber o dinheiro dos bancos da União. Esta questão teve desenvolvimentos subsequentes, mas apenas importa deixar claro que hoje os bancos pagam para armazenar o seu excesso de capital. E preferem pagar a conceder crédito a quem não oferece as garantias necessárias, como se compreende.

As criptomoedas propõem-se a erradicar os custos de armazenamento de dinheiro, por existirem em redes descentralizadas, partilhadas por todos os computadores que nelas desejem participar, não sendo necessário contratar um servidor de software partilhado (vulgo, "*cloud*") para garantir os meios informáticos necessários à sua viabilidade. Ademais, não será necessário recorrer sequer a instituições de crédito para depósito do dinheiro, bastando acesso a um computador e serviços de internet. Deste modo, as criptomoedas apresentam-se como um meio para constituição de reservas de capital sem necessidade de investimento em depósitos ou instrumentos financeiros de baixo risco e, mais importante, sem risco de crédito nem encargos associados[36].

Uma outra utilidade das criptomoedas advém da possibilidade de movimentação de capital num espaço de tempo bem mais reduzido, face àquele a que estamos acostumados. Como vimos, a *Bitcoin* aprova operações a uma média de cada dez minutos. Imagine-se agora o procedimento tradicional para uma instituição de crédito debitar a conta de uma parte e creditar a da contraparte no mesmo

[34] *Vide* https://www.ecb.europa.eu/press/pr/date/2014/html/pr140605_3.en.html (consultado a 18 de outubro de 2019).

[35] "*On 5 June 2014, the ECB Governing Council lowered the Main Refinancing Operation rate to 0.15% and the Deposit Facility (DF) rate to -0.10%. Because banks held significant amounts of excess liquidity during this period, short-term market rates closely tracked the DF rate, effectively making the DF rate the main policy rate. With this decision, the ECB ventured into negative territory for the first time in its history. (...)*". A ideia do BCE foi, na sua essência, penalizar os depósitos por forma a incentivar o "*risk-taking*" dos bancos com grandes concentrações de depósitos. Sobre este tema, *vide* https://www.ecb.europa.eu/pub/economic-research/resbull/2018/html/ecb.rb180213.en.html (consultado a 18 de outubro de 2019).

[36] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 61-63.

valor[37], que, dependendo do valor e da localização geográfica das partes, pode levar dias até ser concretizado. Este processo moroso e desadequado às necessidades do setor financeiro é um dos maiores alvos da digitalização, e os bancos já começaram a agir no sentido de o modernizar[38].

Mas a possibilidade de realização de transferências imediatas[39] não se circunscreve às criptomoedas. Existem hoje *blockchains* que permitem associar um bem, físico ou digital, a uma transferência de criptomoeda, fazendo com que a transferência destas implique necessariamente a transferência do título de propriedade sobre o bem.

Estas tecnologias recorrem usualmente a *colored coins* ("moedas coloridas"), que, pese embora o termo empregue, são verdadeiros *tokens*, uma vez que a cada cor está associado um ativo diferente. Deste modo, todos os utilizadores sabem, por exemplo, que a uma moeda verde corresponde determinada participação no capital social de uma sociedade, uma moeda laranja representa participação no capital social de sociedade diversa, e uma moeda vermelha equivale a uma determinada licença de propriedade intelectual – à obra literária ou musical mais recente de um artista[40]. Estas tecnologias que permitem ligar metadados à transferência de uma criptomoeda justificam a utilização do termo "criptoativos" e são vulgarmente apelidadas de *altcoins*[41].

[37] O chamado "*settlement*" ou "compensação" de operações.

[38] A solução descrita foi adotada pela potência bancária norte-americana, *JPMorgan Chase & Co.*, que, em 14 de fevereiro de 2019, anunciou a criação da sua própria criptomoeda, a *JPM Coin*. Curiosamente, em 2017, o seu CEO, Jamie Dimon, foi um dos primeiros a negar qualquer utilidade às criptomoedas, chegando mesmo a apelidar a *Bitcoin* de "fraude". Hoje, a *JPMorgan Chase & Co.* utiliza a *JPM Coin*, a sua criptomoeda, para realizar transferências instantaneamente através de tecnologia *Blockchain*. Para mais informações, *vide* https://www.jpmorgan.com/global/news/digital-coin-payments.

[39] Leia-se "num espaço médio de dez minutos".

[40] As cores e respetivas funcionalidades ilustradas têm valor meramente exemplificativo.

[41] Abreviatura de "*Alternative Coins*", no sentido em que divergem da criptomoeda original, a *Bitcoin*. A mais famosa e impactante *altcoin* é a rede *Ethereum*, que conta já com uma pletora de diferentes aplicações.

O exposto para as criptomoedas aplica-se também aos criptoativos. Focando-nos na atividade de *trading*[42], a título de exemplo, podemos notar uma diferença abismal entre dois momentos. Atualmente, a tecnologia destinada à execução de ordens de compra e venda chegou a um ponto assustador, onde os pedidos de execução já não são sequer operados pelo Homem. Ao invés, programam-se máquinas, com um tempo de reação esmagadoramente inferior, para comprar e/ou vender dentro de parâmetros definidos. A diferença entre dois pedidos de execução efetuados por máquinas de alta frequência é medida em nanossegundos[43] [44]. Ironicamente, o débito das contas que compraram e crédito das homónimas que venderam, ambas em frações de segundo, levam vários dias a serem processados[45]. Ora, também aqui se prevê um papel para as *blockchains* que se proponham a validar estas operações de modo praticamente instantâneo[46].

Por fim, vemos nos criptoativos uma bênção para os revisores oficiais de contas e reguladores do sistema financeiro. A rastreabilidade associada à condução de operações em tecnologias *blockchain* pode, a nosso ver, facilitar em muito o controlo interno de gestão e o reporte de informação às entidades supervisoras competentes. Mais importante, inviabiliza-se a possibilidade de *cook the books*[47]. Será possível saber, a todo o tempo, qual o estado financeiro de uma sociedade e quais os negócios que correspondem às suas operações na rede. Mitiga-se a necessidade de confiança dos investidores no relatório de gestão e, antes deste, na palavra da administração. Torna-se também possível verificar se as sociedades de facto assumem

[42] Compra e (re)venda de moeda, ou outros produtos financeiros com o objetivo de obtenção de lucro.

[43] Um nanossegundo equivale a 0,000000001 segundos.

[44] Neste sentido, é comum falar-se em *High Frequency Trading*.

[45] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 65.

[46] *Vide* Andrea Pinna/Wiebe Ruttenberg, *Distributed ledger technologies in securities post-trading: Revolution or evolution?*, Banco Central Europeu, *Occasional Paper Series no.* 172, abril 2016, acessível em: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf (consultado a 18 de outubro de 2019), 23-32.

[47] Famosa expressão norte-americana para a alteração fraudulenta de declarações financeiras.

os compromissos que passam ao público (máxime, ambientais) e em que medida estão a investir nos mesmos – tudo se encontra público na rede.

Num universo idealista, onde a adoção destas tecnologias fosse plena, o dever de relatar a gestão e apresentar contas, previsto no artigo 65.º do Código das Sociedades Comerciais, bem como a necessidade de as sociedades serem periodicamente auditadas, estariam simplificados em grande parte, pelo facto de as operações de uma determinada sociedade poderem ser rastreadas e auditadas a todo o tempo e por qualquer *stakeholder*. Os investidores podem saber de antemão se do registo de operações da sociedade resultam relações com agentes poluentes, sancionados pela comunidade internacional, criminosos ou de confiança questionável no mercado. A decisão de participar ou não no capital de uma sociedade poderia ser tomada de um modo muito mais informado e transparente[48].

2. *Smart Contracts*

Os "contratos inteligentes" representam, na nossa opinião, a maior potencialidade jurídica das tecnologias *blockchain*.

A ideia surgiu em 1997, quando o jurista e criptógrafo Nick Szabo, reconhecendo a fragilidade da mera afetação a meios eletrónicos de contratos tradicionais, explicou como sistemas criptográficos mais robustos poderiam dar lugar a softwares capazes de redigir "cláusulas contratuais"[49] e vincular as partes de modo a minimizar ou mesmo extinguir a possibilidade de incumprimento contratual[50].

Com as tecnologias *blockchain 2.0*, máxime a rede *Ethereum*, a ideia conceptualizada por Szabo ganhou expressão. Desde então, surgiram vários tipos de *smart contracts*. Cabe então, em primeira

[48] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 63.

[49] Ou o seu equivalente em linguagem de código.

[50] *Vide* Nick Szabo, *Smart Contracts: Formalizing and Securing Relationships on Public Networks*, First Monday, Volume 2, n.º 9, 1997, acessível em: https://ojphi.org/ojs/index.php/fm/article/view/548/469 (consultado a 18 de outubro de 2019).

instância, analisar o que distingue esta nova forma de celebração contratual das tradicionais cláusulas em papel e suporte digital, como a assinatura digital ou o clique numa *checkbox*, que mais não são do que maneiras de converter um contrato em papel num contrato em suporte informático, sem trazer qualquer tipo de nuance ao conteúdo ou modo de celebração.

Em primeiro lugar, as partes negoceiam os aspetos essenciais do contrato num sistema que os converte em código informático. Como sucede tradicionalmente, o contrato é igual à soma das cláusulas pelas quais as partes optaram. Após finalizado, as partes submetem o contrato à rede em forma de operação (A enviou a B dois *Ether*[51] como pagamento por um determinado bem ou serviço), que é por esta aprovada e inserida num bloco, de modo análogo ao que estudamos para a *Bitcoin*.

Uma vez firmados, os termos de um *smart contract* vão inevitavelmente ser executados, a não ser que as partes tenham previsto a possibilidade de renegociar o contrato. Se nada for acordado em sentido diverso, verifica-se uma de duas situações: ou a parte obrigada cumpre com as disposições do contrato, obtendo a remuneração acordada; ou incumpre com estas e o valor acordado é devolvido à contraparte[52] (se não for acordada outra solução para sanar o incumprimento).

A grande inovação desta tecnologia materializa-se na capacidade de as partes poderem prever várias vicissitudes que possam surgir ao longo da relação contratual, e de decidir os termos em que o contrato se adapta automaticamente na eventualidade de uma ou várias se concretizarem[53].

[51] Moeda subjacente à *blockchain Ethereum*.

[52] *Vide* Aaron Wright/Primavera De Filippi, *Blockchain and the Law: the rule of code*, Harvard University Press, 2018, 74-76.

[53] Por exemplo, preverem que a cada dia de atraso no cumprimento, uma percentagem do valor acordado retorna à carteira digital da parte não culposa; ou que se a parte não disponibilizar um bem no prazo acordado, deve proceder ao envio uma unidade extra. As possibilidades são tantas quanto a imaginação dos intervenientes.

Diferentemente, as partes podem acordar que em caso de incumprimento, parcial ou total, devem renegociar o contrato em termos a definir posteriormente, no momento da renegociação. Deste modo, os sujeitos contratuais podem adaptar o *smart contract* em tempo real às circunstâncias concretas da sua relação.

Em situações em que a aferição do cumprimento contratual seja mais subjetiva[54], os intervenientes podem acordar submeter qualquer disputa à rede, deixando a cargo da totalidade dos utilizadores decidir sobre a existência de incumprimento contratual. Neste caso, os nódulos da rede têm de decidir entre um de dois cenários, aprovando a operação correspondente a esse cenário na rede. A operação que seja aprovada por mais de metade da rede, vencerá a causa.

Um último aspeto merecedor de referência são os *oracles* ("oráculos")[55], termo cunhado pelos programadores para definir uma terceira parte a quem as partes confiam a adaptação do contrato em tempo real, durante toda a relação contratual, e/ou a resolução de litígios. Os oráculos podem ser pessoas ou programas[56], e são capazes de armazenar e transmitir à rede as informações relevantes para esta se adaptar a acontecimentos externos. Se duas partes celebram um contrato de *swap* de taxa de câmbio, vão necessitar de recorrer a um oráculo que esteja ligado à cotação das duas divisas em que o contrato se baseia.

Finda esta breve caraterização, cumpre então analisar de que modo e em que setores podem estes contratos inteligentes inovar.

[54] Não descurando a eterna existência de subjetividade no Direito, referimo-nos a obrigações cujo cumprimento tem uma componente eminentemente subjetiva. Como exemplo, a prestação de serviços de remodelação de uma habitação, em contraposição a situações de aferição menos subjetiva, como seria a obrigação da entrega de um livro – neste segundo caso, o cumprimento da obrigação não pende tanto sobre os critérios pessoalmente adotados pelo sujeito contratante, mas antes pelo bom estado de conservação do objeto.

[55] *Vide* Aaron Wright/Primavera De Filippi, *Blockchain and* cit., 75-83.

[56] A título de exemplo, um medidor de humidade pode ser um oráculo para aferição de secas no âmbito de um contrato de seguro de colheitas. Já o nível de incapacidade de um trabalhador, decorrente de determinado acidente no âmbito de um contrato de trabalho, terá de ser aferido por um médico especialista.

2.1. *Peer-to-peer arbitration*

Em primeiro lugar, é dada às partes a possibilidade de resolução alternativa de litígios através de um meio aparentemente menos custoso e mais célere. Esta *peer-to-peer arbitration*[57] ("arbitragem entre pares") apresenta algumas vantagens face aos modelos tradicionais de arbitragem[58].

Por definição, este mecanismo não necessita nem depende da escolha de árbitros pelas partes, podendo estes ser aleatoriamente selecionados pela rede, ou mesmo serem todos os nódulos desta. Tampouco são necessárias viagens, audiências presenciais e discussões quanto ao tribunal competente ou lei aplicável[59], uma vez que os litígios são dirimidos na rede e pela rede, consoante as regras definidas por esta ou, na ausência destas, pelo voto de cada participante na decisão. A nosso ver, estas particularidades tornam o processo consideravelmente menos moroso.

Quanto aos custos envolvidos, não conseguimos responder da mesma forma – pelo menos para todos os casos. De modo a incentivar os nódulos da rede a participarem na resolução de litígios decorrentes de *smart contracts*, é de prever que as partes tenham de oferecer qualquer tipo de incentivo. Esta lógica poderá levar a que as partes com maiores recursos consigam ver as suas disputas resolvidas em menos tempo e por árbitros melhores, ou, pelo menos, mais empenhados na aplicação da justiça ao caso concreto. Neste sentido, e tendo em conta que o tempo consumido pela arbitragem *peer-to-peer* se prevê muito inferior ao da arbitragem tradicional, não será de admirar que, em alguns casos, os custos dos incentivos a pagar aos nódulos de uma determinada rede, no seu cômputo geral, excedam os dos honorários de três árbitros especializados.

[57] Também apelidada de "*judge-as-a-service*" ou "*arbitration-as-a-service*". Neste sentido, *vide* Aaron Wright/Primavera De Filippi, *Blockchain and*..., 75.

[58] *Vide* Michael Abramowicz, *Cryptocurrency-Based Law*, Arizona Law Review, n.º 58, 2016, acessível em: http://arizonalawreview.org/cryptocurrency-based-law/ (consultado a 18 de outubro de 2019), 405-408.

[59] *Vide* Michael Abramowicz, ob. cit., 405.

Reconhecemos, no entanto, que este problema pode ser facilmente solucionado pela imposição de um limite máximo por incentivo.

2.2. Serviços financeiros

A emergência de *smart contracts* ressoa principalmente no setor financeiro, contribuindo para a sua crescente modernização. A adoção de contratos inteligentes implica mudanças para todos os intervenientes do setor, e não só para os bancos, como seria de pensar. Paralelamente, é comum ouvir-se que a crescente onda de *fintech*[60] e *legal tech* levará à erosão dos bancos. Não partilhamos dessa opinião. Entendemos que os bancos terão de se adaptar a várias tecnologias contemporâneas[61] e de aceitar a perda do monopólio na prestação de determinados serviços. No entanto, cremos que estes desempenham e continuarão a desempenhar um importante papel na economia.

A banca de retalho é talvez o subsetor mais afetado pelos *smart contracts*. Já vimos que o armazenamento de riqueza poderá passar por criptoativos, possivelmente despindo os bancos de uma das suas funções clássicas[62], pelo que não abordaremos a temática neste subcapítulo.

A concessão de crédito e as transferências entre pessoas singulares[63] podem em muito beneficiar da adoção de tecnologias *blockchain*. Através de um *smart contract,* qualquer indivíduo se pode tornar um mutuante. A existência de plataformas descentralizadas onde se permita cruzar procura com oferta de crédito possibilita a celebração de contratos de mútuo à escala mundial e em condições

[60] Abreviatura de "*Financial Technology*".

[61] E, nesta obra, já constatamos que o estão a fazer (cfr.[38]).

[62] No entanto, também constatamos que os bancos já diligenciaram no sentido de não ficarem de fora desta atividade, criando os seus próprios criptoativos. Como tal, não prevemos que opere uma substituição de intervenientes na banca, mas antes a sua abertura a novos participantes.

[63] Trataremos o financiamento de pessoas coletivas no subcapítulo 2.3.

bem mais eficientes do que as atualmente oferecidas pelos bancos[64]. Isto porque os bancos vivem (também) da assimetria de informação entre as partes. Não é comum o mutuário negociar a taxa anual efetiva global ou sugerir alterações às condições gerais impostas pelo banco. Assim o é porque o cliente bancário sabe que, naquela relação contratual, não detém qualquer poder negocial. Caso não aceite a proposta, terá de recorrer a outro banco, que lhe imporá condições igualmente onerosas. Se o mercado mundial de crédito for tornado acessível em tempo real ao comum cidadão, qualquer pessoa poderá financiar-se ou acordar financiar outrem, onde quer que estejam, sem necessidade de confiar na contraparte para o cumprimento do contrato.

Ademais, a completa rastreabilidade das tecnologias *blockchain* permite a qualquer utilizador consultar todas as operações já realizadas pela contraparte, tornando possível a criação de um sistema de classificação[65] de cada chave-pública com base na percentagem de contratos que a mesma incumpriu ou de operações que tentou realizar e lhe foram vedadas pela rede[66]. Esta ideia não é mais do que o cumprimento parcial do dever de *know your customer* (vulgo, "KYC"), imposto a nível europeu[67], legal[68] e regulatório[69] às instituições de crédito. Não pode a *blockchain* almejar substituir o KYC[70], mas, na eventualidade de uma praça global de crédito, torna-se per-

[64] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 71-73.

[65] *Vide* Don Tapscott/Alex Tapscott, ob. cit. 79-82.

[66] Por insuficiência de saldo, por exemplo.

[67] Entre outros, art. 18.º e ss. da Diretiva n.º 2014/17/UE, do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativa aos contratos de crédito aos consumidores para imóveis de habitação e art. 8.º e ss. da Diretiva n.º 2008/48/CE, do Parlamento e do Conselho, de 23 de abril, relativa a contratos de crédito aos consumidores.

[68] Entre outros, art. 16.º e ss. do Decreto-Lei n.º 74-A/2017 de 23 de junho, que transpõe parcialmente a Diretiva 2014/17/UE, relativa a contratos de crédito aos consumidores para imóveis destinados a habitação e art. 10.º do Decreto-Lei n.º 133/2009, de 2 de junho, que transpõe para a ordem jurídica interna a Diretiva n.º 2008/48/CE, do Parlamento e do Conselho, de 23 de abril, relativa a contratos de crédito aos consumidores.

[69] Entre outros, Aviso n.º 4/2017 do Banco de Portugal.

[70] Há imensas componentes deste dever que não podem ser asseguradas através de uma base de dados descentralizada, como a identificação das partes e eventuais beneficiários efetivos, a aferição da sua capacidade e a identificação de casos de simulação e erro. Neste sentido,

tinente que todos os sujeitos tenham acesso ao histórico financeiro das possíveis contrapartes.

Vantagem diversa, mas indissociável da anterior, é a descentralização dos serviços financeiros, máxime dos serviços de pagamento. Os "prestadores de serviços de confiança" perdem relevância num mundo onde a identidade das partes não é elemento essencial à conclusão do negócio jurídico. O inexorável cumprimento ou incumprimento (e a produção dos efeitos acordados para cada hipótese) de um *smart contract* tornam desnecessário averiguar a quem pertence uma determinada chave-pública. Enquanto credores, podemos estar seguros de que a prestação prometida vai ser realizada, ou, não o sendo, de que serão acionadas as medidas corretivas acordadas. Como tal, fica excluído da relação contratual qualquer intermediário, mormente um prestador de serviços de pagamento[71] que pudesse ter como função atestar a identidade das partes e sua solvabilidade, sendo esta última função agora assumida pela *blockchain*. E com a remoção destes terceiros, desaparecem os custos associados às suas comissões.

Este novo tipo de celebração contratual pode ainda aproveitar aos reguladores do sistema financeiro. Para além da transparência, instantaneidade, *timestamping*, e rastreabilidade das *blockchains*, a inexorabilidade associada ao (in)cumprimento dos *smart contracts* permite aos reguladores saber em tempo real onde está o capital das instituições de crédito[72]. Existe ainda a possibilidade de tipificar as obrigações de reporte das entidades financeiras aos respetivos reguladores através de *smart contracts*, associando a coima legalmente prevista à consequência pelo seu incumprimento.

Por tudo isto, cremos que os *smart contracts* podem vir a ser uma importante ferramenta para a gestão do risco associado às operações financeiras[73]. Com a compensação de contas a operar de modo

vide João Vieira dos Santos, *Desafios jurídicos e regulatórios das Initial Coin Offerings*, em Fintech II: Novos Estudos Sobre a Tecnologia Financeira, Almedina, 2019, 305-306.

[71] Na aceção do n.º 11 do artigo 4.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno.

[72] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 66.

[73] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 59.

quase instantâneo e as consequências do incumprimento contratual devidamente acauteladas[74], torna-se possível mitigar de forma significativa o risco de incumprimento da contraparte (ou melhor, os efeitos adversos que daí advenham)[75]. Ao prevenir, no pior dos cenários, os efeitos nefastos da insolvência da contraparte (expressa, na relação *inter partes*, pelo seu incumprimento contratual), nomeadamente através da reversão do pagamento, do qual esta não podia dispor até cumprimento integral do contrato, é possível, pelo menos em abstrato, mitigar o risco sistémico de todo um setor ou economia.

Uma última oportunidade para o sistema financeiro, de cariz mais humanitário, prende-se com a mundialização do acesso a contas bancárias. A verdade é que, pese embora toda a digitalização e *downsizing*[76] no setor bancário, estima-se que, dois mil milhões de pessoas hoje ainda não têm acesso a uma conta bancária[77]. O motivo são os custos de estrutura associados à atividade bancária, que ainda existem a um nível significativo. Nas zonas mais desfavorecidas do planeta, o capital angariado por um banco não lhe permitiria faturar o suficiente para fazer face aos custos de estabelecimento[78]. Ora, as tecnologias *blockchain* permitem a qualquer pessoa com acesso à internet celebrar um *smart contract* para abertura de

[74] Relembre-se que estas são definidas *a priori* no contrato, sendo depois imediatamente executadas aquando da verificação do incumprimento.

[75] Tenhamos por base um contrato de crédito relativo a imóveis (vulgarmente apelidado de "crédito à habitação" ou "crédito hipotecário"). No instante em que o mutuário tentasse utilizar o financiamento obtido para, por exemplo, adquirir um bem de consumo, o *smart contract* anterior seria imediatamente dado como incumprido. Como consequência, as partes haviam estabelecido a reversão do mútuo, pelo que se restituía assim a importância ao mutuante, sendo simultânea e consequentemente vedada a compra do bem de consumo por parte do mutuário.

[76] *Downsizing* define a redução mão-de-obra numa sociedade, normalmente por extinção de postos de trabalho. O termo ficou conhecido em Portugal no pós-crise financeira de 2008, quando os bancos começaram a fechar inúmeras agências e a desenvolver serviços digitais, por forma a cortar nos custos de estrutura.

[77] Quem o diz é Banco Mundial, numa estimativa de 2015, acessível em: http://www.worldbank.org/en/news/press-release/2015/04/15/massive-drop-in-number-of-unbanked-says-new-report (consultado a 18 de outubro de 2019).

[78] Para além da estrutura física, existem custos associados salários, questões regulatórias e legais, licenças, obrigações de reporte, entre muitos outros entraves. Para mais sobre a

conta bancária com qualquer banco do mundo, sem que este tenha de se estabelecer nas imediações do seu cliente. Este é um exemplo de como os bancos podem aproveitar as DLTs para prosperar num mercado financeiro mais inclusivo.

2.3. Economia colaborativa

A economia colaborativa, mais até do que a *blockchain*, é um fenómeno recente com grandes implicações à escala mundial. Na sua essência, baseia-se na lógica de que os proprietários de bens duradouros com uma vida expectável de vários anos apenas os utilizam durante uma parcela desse tempo, o que configura uma decisão economicamente ineficiente[79]. Sob esta égide, são várias as plataformas que temos visto surgir[80] com o objetivo de agregar e cruzar a oferta e procura temporária destes bens, precisamente durante o período em que não estão a ser utilizados pelos respetivos proprietários.

Podíamos arguir que estas plataformas se limitam a replicar serviços já existentes, como sejam os de hotéis ou sociedades de locação de automóveis, mas tal não seria inteiramente correto. A *Uber*, a título de exemplo, calcula o preço do serviço de transporte de passageiros com base em fatores como a localização dos seus vários condutores face à localização do passageiro, o tempo de espera do motorista, a distância do percurso, entre outros. Ademais, oferece serviços de GPS tanto aos seus motoristas como passageiros, para que ambos se assegurem de que estão a percorrer a melhor rota possível, ou a desejada por estes segundos. Por fim, disponibiliza um sistema de classificação de condutores e de reclamação, ambos em

falta de infraestruturas bancárias em zonas mais desfavorecidas, *vide* Don Tapscott/Alex Tapscott, ob. cit., 170-181.

[79] *Vide* John J. Horton/Richard J. Zeckhauser, *Owning, Using and Renting: Some Simple Economics of the "Sharing Economy"*, Harvard Kennedy School Research Working Paper Series, RWP16-007, February 2016, acessível em: https://www.nber.org/papers/w22029 (consultado a 18 de outubro de 2019), 6.

[80] Entre as mais mediáticas, *Uber*, *Airbnb* e *Lime*.

tempo real, no final de cada viagem. Um passageiro a quem tenha sido cobrado tempo de espera indevido ou que não tenha visto a sua rota desejada ser respeitada, pode ser totalmente ressarcido numa questão de minutos, e afetar ativamente a avaliação periódica do condutor que o insatisfez. É nosso entender que o sucesso destas sociedades se ancora no facto de conseguirem contornar os formalismos associados aos negócios de locação tradicionais sem comprometerem as garantias dos consumidores.

No entanto, e pese embora o mérito irrefutável que deles resulta, estes serviços não são completamente eficientes[81]. Todos eles se encontram dependentes de um intermediário, uma contraparte central que aufere comissões dos vários locadores, culminando no aumento do preço para o consumidor final. É, à semelhança do que vimos em tópicos anteriores, precisamente aqui que a *blockchain* e, em específico, os *smart contracts* podem singrar.

Ilustrando novamente com o transporte de passageiros, os contratos inteligentes permitem ao passageiro negociar a viagem pretendida com vários transportadores em simultâneo. Ao utilizador cabe partilhar a sua localização atual e destino almejado, e aos motoristas listar as respetivas ofertas. Em momento posterior, o utilizador opta pela oferta que considera mais vantajosa[82], celebrando um contrato inteligente com a contraparte.

São várias as vantagens que daqui surgem. A mais notável é a ausência de intermediação, que inevitavelmente vai diminuir o preço da viagem. Não menos importante é o facto de a contraprestação reverter totalmente a favor do motorista, que vê agora a chance auferir mais enquanto cobra menos aos respetivos passageiros. A resolução de litígios é também acelerada, operando automaticamente em caso de incumprimento, e pode agora ser negociada pelas partes – a opção por um percurso menos vantajoso pode ape-

[81] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 164-169.

[82] Que não será necessariamente a mais barata, uma vez que entram em conta fatores como o trajeto, conforto e tempo de espera pelo motorista.

nas resultar na redução da contraprestação e não num reembolso total[83].

Por fim, podem as administrações locais beneficiar da vasta quantidade de dados inserida nas várias *blockchains* de serviços agregadores por forma a desenvolver serviços mais adequados às necessidades locais no que concerne a vias de comunicação, alojamento, bem como qualquer outro tipo de infraestruturas[84].

2.4. O caso particular da distribuição de energia

Optamos por conferir autonomia ao caso da distribuição energética, por ser aquele que, dentro dos serviços agregadores de procura e oferta, mais impacto pode ter no quotidiano social.

A diferença, quando confrontada com os exemplos *supra*, está essencialmente no facto de a *blockchain* não se propor só tornar a distribuição de energia mais eficiente, mas a destronar um monopólio.

A distribuição energética é pacificamente tida como um monopólio natural, decorrente dos elevados custos de estrutura associados à atividade. Facilmente se compreenderá que ninguém está disposto a construir uma rede de distribuição de energia que abranja todo o território nacional apenas para concorrer no mercado (ou seja, praticar preços mais baixos aos ideais). Ainda que tal acontecesse, o dispêndio massivo na infraestrutura refletir-se-ia no custo final da energia e o concorrente baixaria os seus preços, resultando inviável qualquer expectativa de sequer compensar o investimento realizado.

[83] A *Arcade City* é uma *blockchain* que visa concorrer com os principais agregadores de serviços de transporte de passageiros nos termos referidos no presente subcapítulo. Cfr. https://arcade.city/.

[84] Nestor M. Davidson/John J. Infranca, *The Sharing Economy and the Upside of Disrupting Local Governance*, Harvard Law Review Blog, 2017, acessível em: https://blog.harvardlawreview.org/the-sharing-economy-and-the-upside-of-disrupting-local-governance/ (consultado a 18 de outubro de 2019).

Neste setor, o papel da *blockchain* centra-se na produção, armazenamento e distribuição de energias renováveis[85]. Num mundo com preocupações ambientais crescentes, é cada vez mais comum vermos habitações equipadas com painéis solares. Estes equipamentos não só ajudam a poupar nos custos energéticos, como conferem aos seus proprietários a possibilidade de vender qualquer excedente produzido. A ineficiência do sistema é introduzida, uma vez mais, pelo intermediário – o distribuidor.

Hoje, é impossível um sujeito vender o seu excedente energético ao vizinho; ao invés, o produtor local vende o seu excedente à sociedade que controla a rede de distribuição de energia que, por sua vez, o venderá ao vizinho deste. Por só poder vender a energia produzida a um comprador (e uma vez que a sua capacidade de armazenamento é limitada), o produtor terá de se sujeitar ao mais ínfimo dos preços.

As vantagens da introdução de *smart contracts* nesta realidade parecem relativamente previsíveis[86]: os produtores podem, na rede de distribuição já instalada (ou seja, sem custos de estrutura), negociar em tempo real o seu excedente energético com vários compradores, o que resulta benéfico para ambas as partes enquanto conseguirem praticar preços inferiores aos do distribuidor tradicional. Estes pequenos produtores conseguem competir com o gigante monopolista pelo facto de existirem perdas energéticas que se acentuam consoante a distância entre o distribuidor e o comprador; ou seja,

[85] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 148-150.

[86] E já existem, embora em pequena escala. A LO3 é uma sociedade de cariz tecnológico que desenvolve medidores de capacidade de produção energética para edifícios; medidores esses capazes de comunicar entre si, graças à tecnologia *blockchain* subjacente ao seu software. Estes instrumentos, capazes de operar nas redes tradicionais de distribuição energética, permitem aos vários utilizadores desta DLT comprar ou vender energia entre si, sem necessidade de qualquer intermediação. Os medidores podem ser programados para comprar ou vender tendo em conta fatores como o melhor preço oferecido ou de modo a produzir a menor perda energética, pelo que não é necessário que os compradores e vendedores estejam constantemente a leiloar. Esta é, para nós, uma das mais arrojadas aplicações jurídicas das tecnologias *blockchain*, pelo impacto que pode criar e pela forma como se propõe a disromper o mercado centenário em que se insere. Para mais informação sobre a LO3, *vide* https://lo3energy.com/.

custará claramente menos ao pequeno produtor vender energia ao seu vizinho do que custa ao distribuidor tradicional, com as suas instalações bem mais longe deste possível comprador, vender-lhe exatamente a mesma quantidade.

O fenómeno suprarreferido, para além de maximizar os ganhos dos produtores e reduzir os custos energéticos dos compradores de energia, pode ainda ser um importante fator para revitalizar e tornar mais atraente o alojamento em localizações tendencialmente menos povoadas – o que se afigura particularmente útil para o panorama português.

Na nossa opinião, o incentivo para a aquisição de painéis solares tenderá a crescer, assim como o valor das habitações com melhor irradiação. Paralelamente, as pessoas procurarão habitação junto de zonas com elevada concentração de produtores de energia, por forma a reduzir os seus custos. Não será certamente só por este facto, mas vemos aqui um importante passo para a concretização de um tão desejado êxodo urbano, uma vez que é no interior do país que estão situadas as maiores oportunidades de benefício da energia solar, dada a ausência de construção em altura e concentração empresarial.

3. *Initial Coin Offerings* ("*ICOs*")

3.1. Conceito e estrutura

As *initial coin offerings* ("ofertas iniciais de moeda") são talvez a aplicação mais frutífera da tecnologia de contabilidade distribuída à data da presente obra[87]. Sumariamente, consistem na oferta pública de um novo criptoativo, cujo pagamento é efetuado através

[87] Na primeira metade de 2018, 21 mil milhões de dólares destinaram-se a financiar projetos em ICOs. Cfr. *EY study: Initial Coin Offerings (ICOs), The Class of 2017 – one year later*, 2018, acessível em: https://www.ey.com/Publication/vwLUAssets/ey-initial-coin-offerings-the-class-of-2017-one-year-later/$FILE/ey-initial-coin-offerings-the-class-of-2017-one-year-later.pdf (consultado a 18 de outubro de 2019), 4.

de criptomoeda ou moeda com curso legal[88]. Desde o surgimento da tecnologia, têm sido o meio primordialmente escolhido para financiar projetos de *blockchain*, a despeito tanto dos meios tradicionais, como o mútuo bancário ou a alienação de participações sociais, como de outros mais recentes, como o financiamento colaborativo[89] [90] [91].

Embora inexista qualquer tipo de regulação (diríamos mesmo que é precisamente por esta inexistir), os usos de mercado obrigam à divulgação de um documento, vulgarmente apelidado de *white paper* ou *token sale term*, que contenha informação quanto ao novo criptoativo, à sua emissão e aos seus desenvolvedores[92].

No que toca ao novo criptoativo, cumpre divulgar parcial ou totalmente o código informático que lhe serve de base, qual a sua função, o modo de funcionamento que os criadores visionam e a *blockchain* no qual está ou irá ser desenvolvido.

No respeitante à emissão, importam fatores como o volume da emissão, o preço e mecanismo de distribuição, todos os quais pesam na avaliação de um investidor prudente. Não menos importância

[88] A grande maioria das ICOs é efetuada através da *blockchain Ethereum* e tem como base a tecnologia *Ethereum Request Comment 20*. Esta harmonização oficiosa da tecnologia utilizada para criar novos criptoativos assegura a sua permutabilidade e permite a inserção em *smart contracts*, também estes maioritariamente desenvolvidos na rede *Ethereum*. *Vide*. AA.VV., *ICOs – The New IPOs? How to fund innovation in the crypto age*, Deloitte Blockchain Institute, 2018, acessível em: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/ICOs-the-new-IPOs.pdf (consultado a 18 de outubro de 2019), 5.

[89] Frequentemente apelidado de *crowdfunding*.

[90] Em Portugal, regulado pela Lei n.º 102/2015, de 24 de agosto, pelo Regulamento da CMVM n.º 1/2016, e pela Lei n.º 3/2018, de 9 de fevereiro.

[91] *Vide* AA.VV., *The ICO Phenomenon and Its Relationships with Ethereum Smart Contract Environment*, Dept. of Mathematics and Computer Science, University of Cagliari, acessível em: https://arxiv.org/ftp/arxiv/papers/1803/1803.01394.pdf; e AA.VV., *Don't Sleep on the ICO – A Taxonomy for a Blockchain-enabled Form of Crowdfunding,* Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018, acessível em: http://ecis2018.eu/wp-content/uploads/2018/09/1465-doc.pdf (consultados a 18 de outubro de 2019), 3-5.

[92] *Vide* Saman Adhami*, Why do businesses go crypto? An empyrical analysis on Initial Coin Offerings,* Journal of Economics and Business, 2018, acessível em: https://doi.org/10.1016/j.jeconbus.2018.04.001 (consultado a 18 de outubro de 2019), 7-9.

tem a equipa que assume o projeto, as suas qualificações e experiência, e o plano de negócios subjacente à criação do criptoativo.

As fases de uma ICO padecem também de uma relativa homogeneidade, mostrando-se pertinente falar em quatro momentos distintos: o pré-anúncio, a oferta, a divulgação e a venda[93].

O primeiro passo consiste na divulgação do documento supramencionado junto de potenciais investidores, para que os desenvolvedores possam medir o nível de interesse do mercado e ajustar o modelo de negócio pretendido às aspirações deste.

Posteriormente, a equipa encarregue do projeto dirige a oferta ao público, enunciando a quantidade de *tokens* a ser emitida, o preço por unidade, o volume máximo da oferta, a finalidade a que se destina o montante que a oferta visa angariar, a sua data e os demais aspetos relevantes (quais os meios de pagamento aceites, por exemplo).

Segue-se um período de divulgação da ICO, que assume especial importância, dado que esta oferta é geralmente (totalmente, à data da presente obra) levada a cabo por *startups*, isto é, sociedades completamente desconhecidas pelo mercado, e sem qualquer obrigação de elaboração ou registo de prospeto que ateste às várias disposições que a lei estatui para proteção dos investidores[94]. A importância desta divulgação acresce ainda pelo facto de as ICOs se dirigirem a pequenos investidores, dispersos mundialmente, ao passo que as ofertas públicas são geralmente endereçadas a investidores institucionais e privados com grande capacidade, bastante mais atentos ao mercado. Como tal, esta fase é vulgarmente subcontratada a sociedades especializadas, que realizam atividades de marketing junto dos fóruns relevantes, durante o período considerado necessário pelos desenvolvedores.

Tudo isto culmina na ICO *stricto sensu* – a emissão e venda dos *tokens*, nos termos e com os objetivos referidos.

[93] *Vide* AA.VV., *ICOs – The New IPOs?* cit., 4.

[94] A titulo de exemplo, cfr. título III do Código dos Valores Mobiliários, máxime artigos 114.º e 115.º.

3.2. ICO vs. IPO

Chegados a este ponto, justifica-se uma palavra sobre os motivos que justificam a elevada afluência[95] deste meio de financiamento. Para tal, mostra-se impreterível que o leitor tenha assente que as ICOs não são, à data desta obra, reguladas por qualquer lei ou entidade. De facto, este é o maior traço distintivo entre esta figura e outras já previstas, como a da oferta pública e o financiamento colaborativo de capital. A possibilidade de as ICOs contornarem muitos dos constrangimentos legais deve-se a esta ausência de previsão e consequente regulação; no entanto, a mesma também pode comportar diversos riscos, como a seu tempo teremos oportunidade de referir.

Não raramente encontramos a ICO como uma *initial public offering*[96] ("IPO") realizada por via de uma *blockchain*. No entanto, estas figuras não são duas faces da mesma moeda o que, consequentemente, leva a que não seja igual optar por uma ou por outra. Na IPO, uma sociedade aliena parte de si em troca de capital. Isto é, ao vender uma determinada percentagem de participação no seu capital, a sociedade está a abdicar (ainda que na mais ínfima percentagem) de parte do seu controlo, abrindo a terceiros a possibilidade de conformar o modo como a mesma agirá desse momento adiante. Estes terceiros visam lucrar com a valorização da sociedade ao longo do tempo, expressa no crescimento do valor por ação e/ou na distribuição de dividendos. É seguro, portanto, concluir que uma IPO se destina a investidores que procuram essencialmente valor.

Os *tokens* emitidos numa ICO, antes de mais, podem não representar qualquer tipo de participação no capital da sociedade emitente. Embora não descure a obtenção de valor por parte dos investidores, a ICO visa essencialmente criar uma rede de *stakeholders*, aumentando a utilidade do *token* a emitir. Tenhamos como exemplo a *Storj*, uma sociedade que criou um serviço de armazenamento tipo *cloud* com base em tecnologia *blockchain*. Qualquer utilizador da

[95] Note-se que não utilizamos o termo "sucesso".

[96] Primeira oferta pública de subscrição por parte de uma sociedade.

plataforma pode alugar espaço no disco rígido dos outros computadores que integram a rede, ou oferecer o seu próprio espaço de armazenamento vago, mediante remuneração. Por forma a tornar possível a prestação deste serviço, a *Storj* criou um *token* de igual nome ("*STORJ*")[97]. Ao oferecer ao público o criptoativo subjacente ao serviço que a sociedade presta, a *Storj* adquiriu, no espaço de dias, inúmeros utilizadores dispostos a locar ou dar em locação o seu espaço de armazenamento no computador. Pelo menos tão importante como o financiamento obtido da venda dos *tokens* é a difusão e valorização do serviço subjacente; isto porque o valor do *STORJ* está diretamente indexado ao do serviço que a sociedade presta. Facilmente se compreenderá que o valor de um *STORJ* será tão mais elevado quantos mais utilizadores do serviço existirem. Inversamente, pense-se que o valor de todos os *STORJs* em circulação será nulo no dia em que a sociedade cesse a prestação do serviço subjacente.

A nosso ver, o investidor numa ICO procura mais utilidade do que propriamente valor, embora ambos caminhem lado a lado. Como tal, concluímos existirem dois tipos distintos de investidores em *initial coin offerings*: os *stakeholders* e os especuladores. Os primeiros, descritos ao longo do parágrafo anterior, visam fazer parte do ecossistema onde o produto oferecido se insere, gozando da utilidade que este se propõe a trazer. Os segundos (também presentes nas IPOs), como em qualquer mercado, investem sem qualquer desejo de fazer parte do referido ecossistema, procurando antes e apenas obter o *token* por um preço que consideram baixo face às suas expectativas de mercado, para que possam obter lucro da sua venda a *stakeholders* ou outros especuladores[98].

[97] Relembre-se a faculdade de os criptoativos serem divisíveis até à oitava casa decimal. Nas palavras de Shawn Wilkinson, Fundador da *Storj*: "*If a user stored a small file and we owed them $0.0001 for that service, it would be impossible to pay them using traditional methods. The STORJ token allows us to do this quickly, with little to no fee, and the necessary granularity*".

[98] João Vieira dos Santos justifica o sucesso das ICOs com base na existência de uma lacuna nos modelos atuais de financiamento societário, opinião meritória que apenas merece a nossa discordância quanto ao termo empregue ("sucesso") uma vez que cremos ser demasiado

3.3. Vantagens das ICOs

Com base no exposto, podemos depreender algumas vantagens da escolha de uma ICO em detrimento de uma IPO.

Em primeiro lugar está a já referida capacidade das ICO conseguirem criar uma rede de *stakeholders* enquanto garantem financiamento, aumentando o valor intrínseco da sociedade emitente e do *token* emitido.

Uma vez que todo o processo tem lugar numa *blockchain*, inexistem custos associados à intermediação da oferta, que se assume como obrigatória nas IPOs[99], e as operações são realizadas de modo quase instantâneo, consoante a velocidade de validação da rede.

Conforme também já referido, a ausência de normativos legais e regulatórios permitem aos empreendedores obter financiamento com base em pouco mais do que uma ideia, o que confere celeridade ao processo e reduz os custos com assessoria jurídica numa fase em que o património da sociedade é geralmente reduzido.

Por fim, tendo em conta o público-alvo das ICOs, os emitentes gozam de uma liberdade muito mais ampla na prossecução do projeto subjacente à emissão. Isto é, como o financiamento provém de pequenas contribuições por múltiplos investidores, inexistem acionistas ou credores controladores que, de modo a assegurarem a rentabilidade do capital investido, condicionam o desenvolvimento do projeto[100].

No reverso da moeda, plasmam-se os problemas de (des)proteção dos investidores a que nos referimos no capítulo seguinte.

cedo para serem tecidos comentários sobre o mérito destas operações. Por esse motivo, cingimos a nossa análise ao aspeto quantitativo das ICOs, razão pela qual nos ancoramos em "afluência". Cfr. João Vieira dos Santos, ob. cit. 301.

[99] Cfr. artigo 113.º do Código dos Valores Mobiliários.

[100] Isto não é dizer que as ICOs se propõem a substituir o capital de risco. Somos da opinião de que ambos podem coexistir, consoante as necessidades de uma sociedade. Se esta procurar estritamente capital, a ICO parece-nos ser a alternativa mais adequada.

III – DESAFIOS DE IMPLEMENTAÇÃO

As barreiras à implementação são o motivo pelo qual as aplicações *blockchain* não se multiplicam com a mesma rapidez das suas teorias. De modo a compreender a sua lenta evolução ao longo dos últimos dez anos, importa conhecer não só as dificuldades técnicas, mas também as de cariz social que, mais ou menos justificadamente, impedem hoje uma maior adoção da *blockchain*.

1. Desafios operacionais

1.1. Capacidade de processamento

Atualmente, a capacidade da *Bitcoin* para processar operações, medida em *transactions per second* ("TPS"), é de 1 TPS, tendo, teoricamente, capacidade para processar até 7 TPS[101]. Um número que se revela relativamente adequado à dimensão atual desta *blockchain*, mas que sem dúvida peca por insuficiência num cenário de adoção global da criptomoeda. A título de comparação, a rede *VISA* processa em média 2.000 TPS, com capacidade para aguentar até 10.000 TPS.

Quer isto dizer que, num mundo onde a rede *Bitcoin* fosse adotada à escala global, a velocidade de aprovação de operações estaria comprometida, pelo que os utilizadores teriam de aguardar, em média, bem mais do que dez minutos pela aprovação dos seus pagamentos. Ainda que não suponhamos este cenário de globalização, dez minutos já revela ser um intervalo temporal desadequado a muitas das práticas quotidianas no presente[102]. Imagine-se o que seria efetuarmos o pagamento de um café em *Bitcoin* e sermos forçados a aguardar até que a operação fosse validada para abandonar o estabelecimento.

[101] *Vide* Melanie Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., 2015, 81.
[102] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 256-257.

Face a um longo, ou pelo menos desajustado, período de incerteza quanto à aprovação das suas operações, presume-se que a maioria dos utilizadores de serviços de pagamento preferirão redes como a *VISA*, ainda que envolvam o pagamento de comissões.

A alternativa lógica seria aumentar o número de TPS da rede[103]. No entanto, se tal vier a ser possível, intensificar-se-á o problema que trataremos em seguida, pelo que continuaríamos despidos de uma efetiva solução para a falta de capacidade de processamento das *blockchains*.

1.2. Dimensão

À data da presente obra, o tamanho total da rede *Bitcoin* é de sensivelmente 209 *gigabytes* ("GB"). Exatamente há um ano atrás, a mesma rede ocupava 162 GB; se distarmos outro ano, pouco mais de 100 GB media[104]. A questão é útil e pertinente: quantos utilizadores têm 209 GB vagos no seu computador para alocar à aprovação de operações na rede? E daqui a um ano? Quantos terão 300 GB?

Na senda do ponto anterior, se a capacidade de processamento de operações da rede *Bitcoin* evoluísse para 2.000 TPS, de modo a poder competir com a *VISA*, estima-se que a *blockchain* cresceria em 3.9 GB por dia[105]. O "*bloat*" ("inchaço", em português), expresso na dimensão crescente de uma rede, é um problema irónico que afeta todas as redes que pretendem ser globais. Irónico porque à medida que uma rede assente em tecnologia de contabilidade distribuída cresce em utilizadores, a sua dimensão aumenta também, até chegar a níveis em que o "inchaço" é de tal forma significativo, que o utilizador comum (a pessoa singular com um computador médio) não a consegue operar no seu equipamento. Por sua vez, o núme-

[103] Atualmente o único método que reconhecemos como capaz de fazê-lo é o fracionamento de redes, uma vez que divide o número de operações pendentes por várias redes, resultando na sua aprovação em simultâneo, embora em redes diferentes. Cfr. nota de rodapé 9.

[104] Fonte: https://www.blockchain.com/pt/charts/blocks-size (consultado a 18 de outubro de 2019).

[105] *Vide* Melanie Swan, ob. cit., 82.

ro de utilizadores diminui, e as recompensas por mineração ficam reservadas aos grandes servidores afetos à atividade, centralizando assim um sistema que, na sua génese, visa a descentralização da economia.

São duas as soluções atualmente propostas para combater o *bloating*. A primeira passa pelo desenvolvimento de novas e mais eficientes tecnologias de compressão de dados. Esta ideia é criticada pelo facto de a compressão pôr em causa a segurança e acessibilidade a dados que uma *blockchain* deve garantir[106]. Solução diversa e que não requer quaisquer desenvolvimentos tecnológicos é a faculdade de optar por *forks* quando a maioria dos utilizadores de uma determinada rede decida que o tamanho desta excedeu o idealmente útil, votando no sentido de criar uma nova rede, com uma dimensão obrigatoriamente menor, uma vez que não incluirá todos os utilizadores da versão anterior. Pese embora a facilidade de adoção, face à alternativa anterior, esta proposta obsta à globalização de qualquer *blockchain*. Os incómodos deste fracionamento são, entre outros, o aumento de volatilidade de todas as criptomoedas (uma vez que o número de utilizadores é menor), a dificuldade em acompanhar o seu valor num determinado momento, bem como a dificuldade de interoperabilidade entre várias *blockchains* – uma vez que as subsequentes bifurcações impossibilitam qualquer compatibilidade entre a criptomoeda original e as várias *altcoins*, e mesmo entre as próprias *altcoins*.

1.3. Insustentabilidade

O dispêndio energético das DLTs que utilizam o mecanismo *Proof-of-Work* é insustentável. Em 2014, Kaminska[107] estimou que o custo energético de manter a rede *Bitcoin* seria equivalente ao de aquecer, em média, 680 casas norte-americanas durante um ano,

[106] *Vide* Melanie Swan, ob. cit., 82-83.

[107] Izabella Kaminska, *Bitcoin's wasted power – and how it could be used to heat homes*, Financial Times, September 5, 2014, acessível em: https://www.ft.com/content/384a349a-32a5-11e4-93c6-00144feabdc0 (consultado a 18 de outubro de 2019).

no mínimo. Em 2015, Schneider disse que eram necessários 100 milhões de dólares anuais para sustentar os 3 mil milhões de dólares em *Bitcoin* existentes à data[108]. E a verdade é que as previsões são de gastos energéticos crescentes[109].

Alguns "mineiros" de *Bitcoin* tentaram contornar os custos energéticos da mineração, movendo os seus servidores para localidades onde o custo energético era menor, mas rapidamente o mercado energético se equilibrou[110].

A única solução expectável passa pela substituição do método *Proof-of-Work* por outros que realizem uma função semelhante, como o *Proof-of-Stake*[111], sendo que esta apenas poderá ser equacionada para redes futuramente constituídas.

1.4. Iliteracia informática

Um dos maiores desafios que atualmente travam a adoção generalizada da *blockchain* é a falta dos conhecimentos técnicos que as operações nesta tecnologia requerem. Não basta saber utilizar um computador; o problema coloca-se pelo facto de as interfaces da maioria das aplicações *blockchain* não serem de fácil compreen-

[108] Nathan Schneider, *After the Bitcoin Gold Rush*, The New Republic, 25 February, 2015, acessível em: https://newrepublic.com/article/121089/how-small-bitcoin-miners-lose-cryptocurrency-boom-bust-cycle (consultado a 18 de outubro de 2019).

[109] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 259-261.

[110] "*With electricity so cheap that most residents use it to heat their homes, the city's consumption exceeded its allocation on several days, Mr. Read explained. As a result, the Municipal Lighting Department had to purchase additional power at much higher prices — a cost it spread across its customers.*" Para mais informação sobre o tema, *vide* Patrick McGeehan, *Bitcoin Miners Flock to New York's Remote Corners, but Get Chilly Reception*, The New York Times, 19 September, 2018, acessível em: https://www.nytimes.com/2018/09/19/nyregion/bitcoin-mining-new-york-electricity.html (consultado a 18 de outubro de 2019).

[111] Neste método, os utilizadores depositam na rede a quantidade de criptomoedas que decidirem e esta decide, com base na quantidade depositada por cada um, qual será o próximo nódulo a adquirir o direito de validar uma operação. A probabilidade de um nódulo ser escolhido é proporcional ao montante do seu depósito. Nas redes baseadas em *Proof-of-Stake*, os termos "mineiros" e "mineração" são substituídos por "aprovadores" e "aprovação".

são para utilizadores sem conhecimentos sobre engenharia ou até mesmo programação[112].

Tenhamos como exemplo as chaves públicas de acesso - que identificam o utilizador nas operações com os seus homónimos - compostas por um conjunto alfanumérico entre vinte e seis e trinca e cinco carateres. O utilizador informático atual está acostumado a identificar-se com o seu nome, correio eletrónico ou uma qualquer alcunha por ele criada (o chamado "*nickname*"). Imagine-se a dificuldade de guardar uma lista de contactos em carateres aleatoriamente gerados. Imagine-se também a medida em que a inserção constante de um conjunto de carateres aleatoriamente gerados, sem qualquer lógica subjacente, propicia o aparecimento de erros nas operações.

Nas palavras de Winklevoss: "*When you go to Google.com you don't type in a string of numbers. You don't type in an IP address. You type in a name, a word that you can remember*"[113].

Mas não se trata apenas da possibilidade de surgirem erros de preenchimento. Qualquer utilizador deve possuir conhecimento, ainda que básico, sobre o modo como as DLTs funcionam e, em específico, sobre a aplicação que deseja utilizar, o que envolve, para além da compreensão de termos como os que foram sendo explicados ao longo da presente obra, a familiarização com interfaces pouco *user-friendly*.

No cômputo geral, no entanto, atribuímos a este obstáculo um peso relativamente pequeno, por acreditarmos que a crescente formação tecnológica da sociedade acabará, em última instância, por tornar banal o conhecimento sobre matérias *blockchain*. Adicionalmente, cremos que as *blockchains* ainda não estão preparadas, de modo algum, para uma adoção generalizada, pelo que existe tempo suficiente para educar futuros utilizadores durante o período de maturação da tecnologia.

[112] Fizemos referência, no âmbito das ICOs, à publicação parcial ou total do código subjacente a aplicações *blockchain*. Este é um aspeto de suma importância para a avaliação da viabilidade do novo *token*. No entanto, são poucos aqueles que conseguem interpretar tal linguagem, essencial a uma tomada de decisão de investimento prudente.

[113] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 255-256.

2. Desafios legais e regulatórios

2.1. Incerteza legal e regulatória

Atualmente, paira uma nuvem de incerteza sobre os aspetos legais e regulatórios em volta das tecnologias *blockchain*. Existe um equilíbrio ténue entre a proteção dos consumidores e o incentivo ao desenvolvimento tecnológico, que nem sempre merece uma resposta unívoca por parte dos Estados. Enquanto os mais conservadores tendem a proibir a utilização de criptoativos e tecnologias *blockchain tout court*, outros, mais liberais, observam cautelosamente o ambiente desregulado, ou criam *regulatory sandboxes*[114], onde podem aferir os benefícios e malefícios da tecnologia[115].

Em todos os casos em que a situação não é resolvida mediante proibição integral, colocam-se várias questões, máxime de perigo para os consumidores, advenientes do vazio legal e regulatório que se faz sentir. Questões essas que não passam indiferentes aos reguladores nacionais e europeus, que já se pronunciaram em diversas oportunidades[116]-[117]-[118]-[119]-[120].

[114] Microcosmos controlados, normalmente com um período de vida finito e definido à partida, onde são testadas inovações tecnológicas sob a supervisão dos reguladores relevantes.

[115] Para um conhecimento mais detalhado das medidas tomadas por cada país na União Europeia e no Espaço Económico Europeu, *vide* Securities and Markets Stakeholder Group, *Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets*, Anexos I e II, acessível em: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (consultado a 18 de outubro de 2019).

[116] *Vide Alerta aos investidores sobre Initial Coin Offerings (ICOs)* da CMVM, acessível em: https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20171103a.aspx (consultado a 18 de outubro de 2019).

[117] *Vide ESMA Statement of 13 November 2017*, acessível em: http://www.cmvm.pt/pt/Cooperacao/esma/DocumentosESMACESR/Documents/esma50-157-828_ico_statement_firms.pdf (consultado a 18 de outubro de 2019).

[118] *Vide EBA Report with advice for the European Commission on crypto-assets*, acessível em: https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf (consultado a 18 de outubro de 2019).

[119] *Vide ESMA Advice on Initial Coin Offerings and Crypto-Assets*, acessível em: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (consultado a 18 de outubro de 2019).

Entre as principais preocupações estão a volatilidade dos criptoativos, a falta de um fundo de garantia para cobertura das perdas dos seus utilizadores, a desinformação resultante da ausência de um prospeto nas ICOs[121], a iliquidez associada a estes instrumentos – uma vez que não têm curso legal, a sua aceitação não é obrigatória[122] –, a dificuldade de identificação da contraparte, a possibilidade de contornar os aparelhos do sistema financeiro para combate ao branqueamento de capitais e financiamento do terrorismo e o risco de fraude, tornado propício pela acumulação de todos estes fatores.

A incerteza legal e regulatória é indubitavelmente, para nós, o maior desafio que as tecnologias *blockchain* enfrentam, uma vez que qualquer evolução que estas sofram pode vir a ser destruída por legislação superveniente. Ou seja, independentemente do nível de desenvolvimento tecnológico que se venha a verificar, é possível que, em última análise, estas tecnologias venham a ser consideradas inúteis, caso os legisladores nacional e europeu assim o decidam.

Obviamente, não nos conseguimos propor a solucionar este problema. Contudo, somos da opinião de que existe, claramente, interesse económico e até social em algumas aplicações da *blockchain*, pelo que nos parece pouco provável que esta venha a ser largamente restringida no Espaço Económico Europeu.

2.2. (In)Segurança

Diferente da incerteza é a insegurança que advém da utilização da *blockchain*. Enquanto a primeira se carateriza pela impossibilidade de prever situações futuras, de modo a optar pela decisão mais racional no presente, a insegurança advém da concretização de cenários que hoje temos como inteiramente possíveis e cuja possibilidade aceitamos quando escolhemos, por exemplo, criar uma carteira de criptoativos. Assemelha-se ao dolo eventual, com a par-

[120] *Vide* Carta Circular n.º 011/2015/DPG do Banco de Portugal, acessível em: https://www.bportugal.pt/cartacircular/0112015dpg (consultado a 18 de outubro de 2019).

[121] Neste sentido, *vide* João Vieira dos Santos, ob. cit. 317-322.

[122] Neste sentido, *vide* João Vieira dos Santos, ob. cit. 310-312.

ticularidade de que o risco assumido é passível de lesar o próprio e não terceiros.

Aqui chegados, recuamos a algumas das considerações iniciais que fizemos, agora munidos de uma visão mais crítica, para identificar alguns dos riscos da *blockchain*.

Dissemos que cada utilizador dispõe simultaneamente de uma chave privada, para aceder à rede, e de uma chave pública para nela se identificar aos seus pares. As ideias subjacentes a estas chaves são as de privacidade e segurança máximas, mas este sistema pode ser ironicamente perverso. Isto porque, em caso de perda da chave privada, o utilizador perde o acesso à rede e, consequentemente, todos os criptoativos que nela detinha. Não existe um nome, correio eletrónico ou qualquer outro tipo de dado pessoal associado às contas, pelo que não há a possibilidade de solicitar o envio de uma nova chave privada/pública[123]. A arquitetura do sistema leva-nos a questionar qual será o ponto de equilíbrio entre segurança e conveniência. Até que ponto queremos estar totalmente seguros – assumindo as consequências que resultam dessa mesma segurança?

Problema diverso, mas relacionado, é o da celebração de negócios jurídicos enfermos de vícios da vontade ou por parte de sujeitos sem capacidade jurídica. A *blockchain* não está hoje preparada para lidar com estas questões. De facto, a pseudonomização que lhe subjaz não só não se dispõe a dirimir, como propícia estes problemas, ignorando todo o processo de formação de vontade das partes contratuais.

Referimos ainda que a divulgação de uma ICO carece da elaboração de qualquer prospeto, o que simplifica e difunde o recurso a este mecanismo de angariação de capital. No reverso da moeda está a prestação aos investidores de informação pouco objetiva, clara ou esclarecedora, e por vezes mesmo incompleta ou fraudulenta. A ausência de regulação leva a que possam ser feitos ICOs para virtualmente qualquer finalidade, sem que os aforradores disponham

[123] Esta possibilidade ganhou mediatismo em 2017, quando um homem tentou escavar um aterro para reaver o disco rígido de que se livrara em 2013. Este disco continha a chave privada de uma carteira que, entretanto, tinha ascendido aos 112 milhões de euros em *Bitcoin*.

de mais provas sobre a sua existência do que aquelas que o oferente decide fornecer. Infelizmente, os ICOs fraudulentos são uma realidade, e prevemos que não se dissipem enquanto a matéria não for regulada.

No campo dos *smart contracts*, falámos na possibilidade de submissão de litígios à rede, para uma justiça mais célere e menos onerosa. Importa agora referir que essa justiça tem um custo: a resolução extrajudicial de litígios com base na "sabedoria popular", isto é, na soma das convicções pessoais de cada utilizador, e não propriamente em fundamentos legais e juízos de equidade. É nosso entender que o recurso a estes mecanismos de resolução alternativa de litígios estará sempre pendente de fatores como a aversão ao risco das partes, o juízo de prognose que estas hajam realizado face à materialidade dos factos e o valor que cada uma atribui à disputa. Só após a ponderação destes três fatores poderão as partes decidir entre uma justiça célere, barata e incerta ou morosa, cara e previsível.

Um último ponto em que gostávamos tocar é o da privacidade financeira[124]. É certo que Nakamoto visionava o anonimato, mas o que criou é melhor expresso por "pseudonimização". De facto, não temos como associar uma determinada chave pública a uma pessoa singular, mas temos acesso a todas as operações realizadas por aquela chave, que agora se propõe a contratar connosco. Ora, esta faculdade é merecedora de algumas críticas da nossa parte, pelo condicionamento das operações futuras de qualquer pessoa a um erro desastroso que possam ter cometido no passado. Reconhecemos que esta não é hoje uma questão de suma relevância, mas sê-lo-á certamente num mundo governado por DLTs.

2.3. Utilização indevida

Como todas as tecnologias, a *blockchain* carece de critérios éticos, limitando-se a servir os dos seus utilizadores. Nesse sentido,

[124] *Vide* Aaron Wright/Primavera De Filippi, *Blockchain and...,* 58-59.

não faltarão certamente exemplos de quem esteja disposto a subverter esta tecnologia, desenhada para otimizar o mercado, num instrumento de perversão do sistema.

O maior destes casos, à data desta obra, foi certamente a "*Silk Road*", um mercado negro de substâncias ilícitas a operar com base na rede *Bitcoin*, entre fevereiro de 2011 e outubro de 2013. A *Silk Road* baseou-se na pseudonomização conferida pela rede para receber pagamentos. Os produtos eram entregues via correio e aos vendedores era fornecido um guia sobre como evitar a deteção pelos órgãos de polícia criminal[125]. A *Silk Road* operava como plataforma agregadora de compradores e vendedores, ficando com uma comissão sobre cada operação realizada – uma espécie de *Uber* do comércio ilícito.

O seu surgimento durante a génese da *blockchain*[126] serviu para que a mesma fosse automaticamente desacreditada aos olhos de grande parte da população. Os restantes ainda hoje receiam que a tecnologia seja utilizada para fins ilícitos.

Os defensores da tecnologia, por sua vez, apontam a total rastreabilidade das operações realizadas como um meio indicado para prevenir e combater o crime. Outros argumentos apresentados incluem o facto de nenhuma tecnologia ser completamente segura e de que a *blockchain* é tão propícia à fomentação de fins sociais como de condutas ilícitas[127].

Em última instância, os argumentos a favor da tecnologia merecem a nossa concordância, ainda que parcial. Embora sejamos da opinião de que a proibição com base no medo, quando existem potencialidades a explorar, seja incorreta, reconhecemos que os meios atuais de prevenção e combate aos mais variados ilícitos criminais não estão preparados para lidar com uma economia descentralizada. Os mesmos problemas regulatórios, de infraestrutura e literacia merecem aqui aplicação; apenas num mundo onde a tecnologia esteja devidamente regulada e a população (incluindo os órgãos de

[125] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 275-276.

[126] Na altura, os termos *blockchain* e *Bitcoin* eram praticamente coincidentes, uma vez que a rede *Ethereum*, impulsionadora da *blockchain* 2.0, apenas surgiu em meados do ano 2015.

[127] *Vide* Don Tapscott/Alex Tapscott, ob. cit., 277.

polícia criminal) devidamente instruída será possível balancear as vantagens e os contratempos da *blockchain*, por forma a ser tomada uma decisão justa.

Na nossa opinião, vincamos a ideia de que a inovação não deve ser travada pelo medo da perversão tecnológica, antes pelo contrário – a perversão de uma tecnologia reclama meios de prevenção e reação, apresentando-se como uma nova oportunidade de inovação.

Bibliografia

AA.VV., *Don't Sleep on the ICO – A Taxonomy for a Blockchain-enabled Form of Crowdfunding,* Twenty-Sixth European Conference on Information Systems (ECIS2018), Portsmouth, UK, 2018, acessível em: http://ecis2018.eu/wp-content/uploads/2018/09/1465-doc.pdf (consultado a 18 de outubro de 2019).

AA.VV., *EY study: Initial Coin Offerings (ICOs), The Class of 2017 – one year later*, 2018, acessível em: https://www.ey.com/Publication/vwLUAssets/ey-initial-coin-offerings-the-class-of-2017-one-year-later/$FILE/ey-initial-coin-offerings-the-class-of-2017-one-year-later.pdf (consultado a 18 de outubro de 2019).

AA.VV., *ICOs – The New IPOs? How to fund innovation in the crypto age*, Deloitte Blockchain Institute, 2018, acessível em: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/Innovation/ICOs-the-new-IPOs.pdf (consultado a 18 de outubro de 2019).

AA.VV., *Legal Technology Vision*, Signapore Academy of Law, 2017, acessível em: https://www.sal.org.sg/Resources-Tools/Legal-Technology-Vision (consultado a 18 de outubro de 2019).

AA.VV., *The ICO Phenomenon and Its Relationships with Ethereum Smart Contract Environment*, Dept. of Mathematics and Computer Science, University of Cagliari, acessível em: https://arxiv.org/ftp/arxiv/papers/1803/1803.01394.pdf (consultado a 18 de outubro de 2019);

Abramowicz, Michael, *Cryptocurrency-Based Law*, Arizona Law Review, n.º 58, 2016, acessível em: http://arizonalawreview.org/pdf/58-2/58arizlrev359.pdf (consultado a 18 de outubro de 2019).

Adhami, Saman, *Why do businesses go crypto? An empyrical analysis on Initial Coin Offerings,* Journal of Economics and Business, 2018, acessível em: https://doi.org/10.1016/j.jeconbus.2018.04.001 (consultado a 18 de outubro de 2019).

Banco Central Europeu, *ECB introduces a negative deposit facility interest rate*, *press release* 5 de junho de 2014, acessível em: https://www.ecb.europa.eu/press/pr/date/2014/html/pr140605_3.en.html (consultado a 18 de outubro de 2019);

CMVM, *Alerta aos investidores sobre Initial Coin Offerings (ICOs)*, acessível em: https://www.cmvm.pt/pt/Comunicados/Comunicados/Pages/20171103a.aspx (consultado a 18 de outubro de 2019).

Correia, Francisco Mendes, *A tecnologia descentralizada de registo de dados (Blockchain) no sector financeiro*, em "*Fintech: Desafios da Tecnologia Financeira"*, Almedina, 2019.

Davidson/ Infranca, Nestor M./John J., *The Sharing Economy and the Upside of Disrupting Local Governance*, Harvard Law Review Blog, 2017, acessível em: https://blog.harvardlawreview.org/the-sharing-economy-and-the-upside-of-disrupting-local-governance/ (consultado a 18 de outubro de 2019).

Santos, João Vieira, dos *Desafios jurídicos e regulatórios das Initial Coin Offerings*, em "*Fintech II: Novos Estudos Sobre a Tecnologia Financeira*", Almedina, 2019.

EBA, *Report with advice for the European Commission on crypto-assets*, acessível em: https://eba.europa.eu/documents/10180/2545547/EBA+Report+on+crypto+assets.pdf (consultado a 18 de outubro de 2019).

ESMA, *Advice on Initial Coin Offerings and Crypto-Assets*, acessível em: https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf (consultado a 18 de outubro de 2019);

– *Statement of 13 November 2017*, acessível em: http://www.cmvm.pt/pt/Cooperacao/esma/DocumentosESMACESR/Documents/esma50-157-828_ico_statement_firms.pdf (consultado a 18 de outubro de 2019).

Horton/ Zeckhauser, John J./Ricard J., *Owning, Using and Renting: Some Simple Economics of the "Sharing Economy"*, Harvard Kennedy School Research Working Paper Series, RWP16-007, February 2016.

Kaminska, Izabella, *Bitcoin's wasted power – and how it could be used to heat homes*, Financial Times, 5 de setembro, 2014, acessível em: https://www.ft.com/content/384a349a-32a5-11e4-93c6-00144feabdc0 (consultado a 18 de outubro de 2019).

Kerikmäe/Hoffmann/Chochia, Tanel/Thomas/Archill, *Legal Technology for Law Firms: Determining Roadmaps for Innovation*, Croatian International Relations Review, Vol. 24, n.º 81, 2018, acessível em: https://hrcak.srce.hr/199994 (consultado a 18 de outubro de 2019).

McGeehan, Patrick, *Bitcoin Miners Flock to New York's Remote Corners, but Get Chilly Reception*, The New York Times, 19 de setembro, 2018, acessível em: https://www.nytimes.com/2018/09/19/nyregion/bitcoin-mining-new-york-electricity.html (consultado a 18 de outubro de 2019).

McGinnis/ Pearce, John. O./Russel G., *The great disruption: how machine intelligence will transform the role of lawyers in the delivery of legal*

services, Fordham Law Review n.º 82, 2014, acessível em: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5007&context=flr (consultado a 18 de outubro de 2019).

Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, acessível em: https://bitcoin.org/bitcoin.pdf (consultado a 18 de outubro de 2019).

Pinna/ Ruttenberg, Andrea/Wiebe, *Distributed ledger technologies in securities post-trading: Revolution or evolution?*, Banco Central Europeu, Occasional Paper Series, n.º 172, abril 2016, acessível em: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf (consultado a 18 de outubro de 2019).

Praduroux/De Paiva/Di Caro, Sabrina/Valeria/Luigi, *Legal Tech Start-ups: State of the Art and Trends*, Universidade de Turim, 2016, acessível em: http://vcvpaiva.github.io/includes/pubs/2016-legal.pdf (consultado a 18 de outubro de 2019).

Schneider, Nathan, *After the Bitcoin Gold Rush*, The New Republic, 25 de fevereiro, 2015, acessível em: https://newrepublic.com/article/121089/how-small-bitcoin-miners-lose-crypto-currency-boom-bust-cycle (consultado a 18 de outubro de 2019).

Securities and Markets Stakeholder Group, *Advice to ESMA: Own Initiative Report on Initial Coin Offerings and Crypto-Assets*, acessível em: https://www.esma.europa.eu/sites/default/files/library/esma22-106-1338_smsg_advice_-_report_on_icos_and_crypto-assets.pdf (consultado a 18 de outubro de 2019).

Swan, Melanie, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., 2015.

Szabo, Nick, Smart Contracts: *Formalizing and Securing Relationships on Public Networks*, First Monday, Volume 2, n.º 9, 1997, acessível em: https://ojphi.org/ojs/index.php/fm/article/view/548/469 (consultado a 18 de outubro de 2019).

Tapscott, Don Alex, *Blockchain Revolution*, Portfolio Penguin, 2.ª edição, 2018.

Wright/De Filippi, Aaron /Primavera, *Blockchain and the Law: the rule of code*, Harvard University Press, 2018;

– *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 2015, acessível em: http://ssrn.com/abstract=2580664 (consultado a 18 de outubro de 2019).