REGULAÇÃO DOS NEGÓCIOS DE TRANSMISSÃO DE CRIPTOATIVOS, COM FOCO NA *BLOCKCHAIN*

Dissertação de Mestrado em Direito e Prática Jurídica com especialização em Direito Civil pela Faculdade de Direito da Universidade de Lisboa, sob a orientação do Senhor Professor João de Oliveira Geraldes

Matilde Esteves Chefe

Lisboa, março de 2025

Índice

1. AGRADECIMENTOS

Aos meus pais, Patrícia e Joaquim, que sempre me apoiaram na concretização dos meus sonhos e me permitiram estar hoje nesta posição tão privilegiada.

Ao meu namorado, Alexandre, por estar sempre ao meu lado nos momentos mais difíceis desta jornada com as suas palavras atenciosas.

Às minhas amigas, Rita, Maria Carolina, Maria Inês e Ana Gabriella que estão também no processo de redação das suas dissertações e foram ajudas preciosas tanto nos a nível técnico como emocional. Quero agradecer à minha amiga Catarina que, estando também dentro da área jurídica, compreende os desafios particulares desta tarefa e tinha sempre uma palavra útil.

Ao resto da minha família, em particular à minha prima Julieta, que realizou também esta caminhada no seu tempo e tranquilizou as minhas ansiedades ao longo da pesquisa.

Ao meu orientador, Senhor Professor João de Oliveira Geraldes, que me apoiou na redação desta dissertação com as suas recomendações e palavras sábias.

2. LISTA DE ABREVIATURAS

CC – Código Civil

CdVM – Código dos Valores Mobiliários

CFPB – *Consumer Financial Protection Bureau*

CMVM – Comissão do Mercado de Valores Mobiliários

CSC – Código das Sociedades Comerciais

DLT – *Distributed ledger technology*

DMIF II – Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros

EBA – *European Banking Authority*

EFTA – *Electronic Fund Transfer Act*

ESMA – *European Securities Markets Authority*

ICO – *Initial Coin Offering*

LCE – Lei n.º 16/2022, de 16 de agosto, relativa às comunicações eletrónicas

NFT – *Non-Fungible Token*

Regulamento MiCA – Regulamento UE 2023/1114 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo aos mercados de criptoativos

3. RESUMO

Na última década, temos assistido ao crescimento exponencial do mercado de criptoativos e tal exige a definição de um quadro jurídico com vista a regular os diversos aspetos que envolvem a transação deste tipo de ativos.

Existindo um novo conjunto de normas regulamentares a aplicar aos criptoativos, o Regulamento MiCA, será necessário compreender quais os temas que deveriam ser tratados de forma mais atenta por este instrumento e quais os temas que deverão ser deixados à discricionariedade das partes.

Esta investigação tem, assim, como objetivo principal a determinação do regime aplicável nomeadamente à formação, modificação e transmissão de criptoativos. De forma a alcançar esse objetivo, propomo-nos a realizar um estudo do anterior e do atual panorama normativo, tanto a nível europeu como português, em matéria de criptoativos; uma análise do funcionamento da *blockchain* e as suas principais características; uma comparação entre os elementos formais e substanciais de um *smart contract* em relação a um contrato tradicional de forma a determinar se existem semelhanças suficientes para alegar uma equiparação entre as duas realidades e, por fim, uma análise das hipóteses de direito aplicável no que diz respeito a aspetos contratuais e extracontratuais que sejam relevantes nesta sede.

Palavras-chave: *blockchain*; transmissão; criptoativo; descentralização; *smart contract*.

4. ABSTRACT

In the last decade, we have witnessed the impressive growth of the crypto-assets market and that demands the determination of a set of rules to regulate various aspects regarding these goods, specifically their transaction.

With the definition of a new set of norms to regulate a vast majority of cryptocurrency related subjects, the Regulation MiCA, it is our job to analyse which topics were to be reserved to said regulation and which topics should be left to the discretion of the contractual parties.

This investigation's primary goal is to figure out which regulation applies to the formation, modification and transmission of cryptocurrency. To achieve that goal, we need to analyse the previous and current European and Portuguese regulatory maps regarding this topic, then we need to study the environment surrounding blockchain platforms and their characteristics, compare the formal and material elements of smart contracts versus traditional contracts to determine if there are enough similarities to consider them actual contracts and lastly, we need to perform an analysis of the possible rules applicable to the contractual and non-contractual aspects that are relevant in this field.

Keywords: blockchain; transmission; crypto-asset; decentralization; smart contract.

5. APRESENTAÇÃO DA PROBLEMÁTICA

1. Com o crescimento do mercado de criptoativos, surge a necessidade de desenvolver um regime específico para os diversos aspetos que envolvem a transmissão deste tipo de ativos.

Com esse objetivo em mente, o primeiro passo a tomar nesta investigação será analisar o fenómeno de crescimento dos criptoativos e estabelecer de que forma é que a questão tem sido tratada tanto no plano interno como externo. Iremos analisar os vários tipos de regras, desde a classificação dos criptoativos, à sua emissão, passando pelas condições que os prestadores de serviços desses ativos deverão respeitar, etc.

O segundo passo será explorar o funcionamento da tecnologia *blockchain,* em especial as características de descentralização, anonimato, verificabilidade e imutabilidade que a definem e a forma como essas características podem influenciar a concretização de um negócio.

Na procura de um regime de transmissão para os criptoativos, fará sentido também fazer um breve enquadramento de Direito Internacional Privado de forma a avaliar em que termos será possível aplicar o direito português a estes casos. Com esse enquadramento em mente, o próximo passo será explorar o tópico do negócio jurídico inserido no contexto do direito contratual português. Cabe-nos analisar os temas centrais desta temática, nomeadamente o acordo entre as partes, a capacidade jurídica para a celebração de negócios, os requisitos formais, a interpretação, a modificação e o incumprimento, estabelecendo comparações entre o contrato tradicional e o *smart contract* de forma a determinar uma possível equiparação entre as duas conjunturas.

Após explorar estes aspetos nas duas realidades contratuais, cabe analisar em específico o regime da transmissão por via do contrato de compra e venda, novamente estabelecendo comparações entre o sistema tradicional e o sistema digital descentralizado. O enriquecimento sem causa surge também dentro deste tópico, tendo em conta a sua proximidade temática e relevância específica num contexto em que a identidade dos intervenientes é encriptada.

2. De forma a resumir a ordem de trabalhos acima apresentada decidimos identificar algumas questões às quais pretendemos responder:

1. Quais as soluções apresentadas, tanto pelo direito português como pelo direito europeu, para regular os vários aspetos essenciais que envolvem a transação deste tipo de ativos?
2. Sendo os *smart contracts* uma das formas de transmissão dos criptoativos, que semelhanças podemos apontar entre este tipo de contratos e os contratos tradicionais? É possível considerar um *smart contract* um verdadeiro contrato?
3. Na ausência de normas regulamentares europeias, qual será o direito a aplicar às obrigações que irão surgir nesta sede? Com base em que normas de conflito é que podemos determinar o direito a aplicar nesta sede?
4. De que forma é que os diversos elementos característicos da *blockchain*, em especial o elemento de anonimato e da imutabilidade, podem afetar a aplicação de institutos de direito civil que afetam o curso de um clausulado contratual?
5. A transmissão de criptoativos poderá ser regulada pelas regras de compra e venda? De que forma é que o objeto deste tipo de transmissão se assemelha a outros já regulados pelo nosso sistema?
6. Havendo uma situação de enriquecimento, será possível aplicar este instituto aos *smart contracts*? Em que medida é que o elemento do anonimato pode dificultar esta aplicação?

6. O CRESCIMENTO DO MERCADO DE CRIPTOATIVOS E PROBLEMAS LEVANTADOS

6.1. Direito português

1. Como sabemos, o crescimento do mercado dos criptoativos criou a necessidade de determinar o regime mais adequado a aplicar a este tipo de ativos. Num momento anterior à aprovação da MiCA, cada ordenamento nacional tinha de determinar, dentro do seu sistema, qual era o conjunto de normas que melhor se enquadrava nesta nova realidade. Em Portugal, esta temática começou a ser explorada em 2017[1].

No ordenamento jurídico português, o autor JOÃO VIEIRA DOS SANTOS apresentou duas possibilidades para qualificar os criptoativos na era pré-MiCA: qualificação como moedas ou como valores mobiliários[2].

2. Como sabemos, no direito português não existe um conceito de moeda, sendo necessário, para efeitos de densificação do conceito, encontrar os casos em que o legislador atribuiu consequências jurídicas relevantes ao desempenho de funções monetárias. Esses bens serão designados de moedas para efeitos jurídicos[3].

Uma das características essenciais para a qualificação como moeda é a obrigatoriedade de aceitação. Isto é, o credor não pode justificar a recusa de notas e moedas em euros com motivos atinentes ao objeto mediato da obrigação, ou seja, à qualificação das espécies monetárias como moeda[4]. O mesmo não sucede com os criptoativos. Mesmo que haja quem aceite os criptoativos como objeto mediato de cumprimento de uma obrigação, tal é feito numa base voluntária e não devido à obrigatoriedade de aceitação[5].

---

[1] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, pp. 45 e 47; LAURA ABREU CRAVO, "Regulação dos criptoativos na era pré MiCA", em *MiCA: Estudos sobre a nova regulação europeia de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, p. 22.
[2] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, pp. 45 e 47.
[3] *Idem*, p. 45.
[4] *Ibidem*.
[5] *Idem*, pp. 46 e 47.

Alguns criptoativos, antes da entrada em vigor do Regulamento MiCA, eram classificados como moeda eletrónica, sendo esta definida pelo Decreto-lei n.º 91/2018, de 12 de novembro, decreto este que aprova o Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica. Estes criptoativos eram definidos como um *"valor monetário armazenado eletronicamente, inclusive de forma magnética, representado por um crédito sobre o emitente e emitido após receção de notas do banco, moedas e moeda escritural, para efetuar operações de pagamento e que seja aceite por pessoa singular ou coletiva diferente do emitente da moeda eletrónica"*[6].

Deste modo, os criptoativos eram classificados como moeda eletrónica se o seu valor estivesse associado ao valor de uma moeda em curso legal. Se correspondessem, por exemplo, ao euro, as entidades que emitem os criptoativos deviam registar-se como instituições de moeda eletrónica junto do Banco de Portugal[7].

3. Outro caminho possível foi a identificação deste tipo de ativos com os valores mobiliários. Dentro do âmbito dos instrumentos financeiros, temos os instrumentos derivados, os monetários, licenças de emissão que podem ser consideradas instrumentos de curto prazo, e os valores mobiliários, instrumentos de médio e longo prazo. Uma vez que grande parte dos criptoativos têm uma durabilidade de longo prazo ou geralmente indeterminada, será de excluir a classificação como instrumentos monetários e de aplicar a classificação como valores mobiliários[8].

Relativamente aos valores mobiliários, os seus critérios de qualificação no direito português encontram-se enumerados no artigo 1.º do CdVM. Neste artigo, estão enumerados os tipos de valores mobiliários, nas alíneas a) a f). Não obstante, a alínea g) desse mesmo artigo reproduz um princípio de atipicidade de valores mobiliários[9]. Nesta alínea, estão elencados os critérios tipológicos positivos para a qualificação de valores mobiliários, estabelecendo-se que os valores mobiliários são *"documentos representativos de situações jurídicas homogéneas, desde que sejam suscetíveis de transmissão em mercado"*.

---

[5] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 46.
[6] *Idem,* pp. 46 e 47.
[7] *Idem*, p. 47.
[8] *Ibidem*.
[9] PAULO CÂMARA, *Manual de Direito dos Valores Mobiliários*, 4ª ed., Almedina, 2018, p. 142.

Como primeiro critério, os valores mobiliários devem ser um documento. Neste enquadramento, deverá considerar-se a noção lata de documento do artigo 362.º do CC, podendo o documento ser em papel ou eletrónico (artigo 2.º, alínea a) do Decreto-Lei n.º 290-D/99, de 2 de agosto), desde que se respeite o princípio da unidade da forma em cada emissão. Os criptoativos preenchem este critério por corresponderem a documentos eletrónicos[10].

Como segundo critério, as situações jurídicas representadas devem ser homogéneas, implicando que as mesmas sejam fungíveis e, consequentemente, que os valores mobiliários também o sejam, de forma a terem aptidão para circular no mercado. Relativamente aos criptoativos, a homogeneidade apenas será um problema se forem atribuídos direitos e obrigações diferentes a cada criptoativo emitido numa ICO. Geralmente, tal não sucede, uma vez que a homogeneidade dos criptoativos é promovida pelos emitentes/oferentes, de forma a garantirem a sua liquidez no mercado secundário[11].

Como terceiro critério, temos a suscetibilidade de transmissão em mercado que deverá ser apreciada em abstrato. Segundo PAULO CÂMARA,

> *"não precisa de se exigir que, em concreto, essa transmissibilidade esteja assegurada. Assim, para avaliar a potencialidade transmissiva de um instrumento há que atender ao respetivo regime supletivo, quanto a saber se deste não resultam embaraços ou constrangimentos a uma circulação fluída. Sendo a resposta negativa, este requisito deve ter-se por verificado"*[12].

Os criptoativos preenchem tipicamente este critério de transmissibilidade. Apenas se for tecnicamente impossível a transmissão é que podemos concluir pela não verificação do critério de suscetibilidade de transmissibilidade. Não nos podemos esquecer também da negociabilidade dos criptoativos em mercado, isto é, os criptoativos devem ser transacionáveis na base do encontro sobre a oferta e procura exclusivamente em relação ao respetivo preço, sem negociação individualizada de outras condições[13].

---

[10] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, pp. 47 e 48.
[11] *Idem*, p. 48.
[12] PAULO CÂMARA, *Manual de Direito dos Valores Mobiliários*, 4ª ed., Almedina, Coimbra, 2018, p. 120.
[13] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, pp. 48 e 49.

Relativamente ao último critério, os valores mobiliários devem incorporar ou representar posições jurídicas, especialmente, direitos e deveres de natureza patrimonial e privada, podendo assumir uma natureza complexa e variável. Nos criptoativos, os direitos e deveres dos seus titulares estão previstos no protocolo da *blockchain* criada[14]. Os criptoativos são representações digitais de situações jurídicas. Existem situações em que estes não representam situações jurídicas, nomeadamente que tenham apenas a finalidade de servir de meio de troca[15].

Deste modo, para JOÃO VIEIRA DOS SANTOS, era possível qualificar os criptoativos como valores mobiliários sempre que se criar uma situação jurídica entre a emitente/oferente e os titulares, após a primeira relação contratual de transmissão, sendo que a situação jurídica que emerge da titularidade dos criptoativos confere direitos e/ou deveres de natureza patrimonial e privada aos seus titulares[16].

4. Em 2018, a CMVM, com vista a erradicar dúvidas em matéria de qualificação, publicou um comunicado dirigido às entidades envolvidas no lançamento de ICOs que dizia respeito à qualificação jurídica dos *tokens*. Nos esforços de desenvolver esta qualificação, a CMVM interpreta o artigo 1.º do CdVM e determina que se deverão encontrar cumulativamente preenchidas as seguintes condições para que se possa qualificar um *token* como valor mobiliário[17]:

1. *Um token é um valor mobiliário caso seja um documento representativo de uma ou mais situações jurídicas de natureza privada e patrimonial (i.e. direitos e deveres);*
2. *(...) A(s) situação(ões) jurídica(s) representada(s) seja comparável com valores mobiliários típicos.*
3. *Para efeitos do disposto no número anterior, deve normalmente considerar-se a previsão, nas informações disponibilizadas pelo emitente, de elementos dos quais possa decorrer uma vinculação do emitente à realização de condutas das quais resulte uma expetativa de retorno para o investidor, como sejam:*

[14] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 49.
[15] *Ibidem*.
[16] *Idem*, p. 50.
[17] LAURA ABREU CRAVO, "Regulação dos criptoativos na era pré MiCA", em *MiCA: Estudos sobre a nova regulação europeia de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, pp. 24 e 25.

- *Direito a um rendimento (por exemplo, se o token conferir direito a lucros ou a um juro);*
- *Prática de atos por parte do emitente ou entidade relacionada adequados à incrementação do valor do token (...).*

As situações jurídicas relevantes deverão ter determinado conteúdo patrimonial, ou seja, a situação deverá referir-se a direitos, deveres, ónus e/ou sujeições, excluindo do conceito de valores mobiliários os criptoativos que sejam exclusivamente aptos a serem utilizados como meio de pagamento ou sejam um ativo em si mesmo[18].

5. Independentemente destas considerações, com o surgimento da legislação europeia, essa prevalece na regulação deste tipo de ativos e o direito português só era aplicável subsidiariamente.

6.2. Direito europeu

1. Atualmente, a principal fonte de Direito em matéria de criptoativos é o Regulamento Europeu relativo aos mercados de criptoativos, mais conhecido por MiCA, aprovado em 31 de maio de 2023, cujos Títulos III e IV entraram em vigor em junho de 2024, tendo os Títulos I, II, V, VI e VII entrado em vigor em dezembro de 2024. Com o surgimento deste quadro regulamentar a nível europeu, o direito português será apenas aplicado de forma subsidiária.

O Regulamento aplica-se à emissão, oferta pública e admissão à negociação de criptoativos, bem como à prestação de serviços relacionados com criptoativos. Esta legislação visa proporcionar clareza e segurança jurídicas aos emitentes de criptoativos e aos prestadores de serviços de criptoativos. Visa impulsionar a inovação, preservando a estabilidade financeira e protegendo os investidores dos riscos.

[18] LAURA ABREU CRAVO, "Regulação dos criptoativos na era pré MiCA", em *MiCA: Estudos sobre a nova regulação europeia de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, pp. 24 e 25.

6.2.1. Contextualização

1. A União tinha um interesse político no desenvolvimento e adoção de tecnologias transformadoras no setor financeiro, incluindo cadeias de blocos (*blockchain*) que se encontram dentro do conceito mais abrangente de DLT. A ausência de um quadro geral da União em matéria de criptoativos poderia conduzir a uma falta de confiança dos consumidores nesses ativos que iria, por sua vez, prejudicar o desenvolvimento deste mercado. A inexistência desta regulamentação poderia ainda conduzir a uma fragmentação regulamentar nesta matéria.

2. Assim, a Comissão Europeia, no dia 24 de setembro de 2020, publicou uma proposta de Regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos que foi objeto de muita atenção mediática e académica. A 20 de abril de 2023, foi aprovada a posição do Parlamento Europeu tendo em vista a adoção do Regulamento (UE) 2023/1114 oido Parlamento Europeu e do Conselho relativo aos mercados de criptoativos. A 31 de maio de 2023, foi aprovado o Regulamento (EU) 2023/1114 do Parlamento Europeu e do Conselho de 31 de maio de 2023 relativo aos mercados de criptoativos e que altera os Regulamentos (EU) n.º 1093/2010 e (EU) n.º 1095/2010 e as Diretivas 2013/36/EU e (EU) 2019/1937.

Procedeu-se assim à criação de um regime relativamente abrangente a aplicar à esmagadora maioria dos criptoativos com uma lista de objetivos extensa.

6.2.2. Objetivos

1. O Regulamento estabelece regras uniformes, como forma de garantir a segurança jurídica, para os emitentes de criptoativos que ainda não foram regulamentados por outros atos da União Europeia em matéria de serviços financeiros e para os prestadores de serviços desses mesmos criptoativos. Visa apoiar a inovação e concorrência leal, garantindo simultaneamente um elevado nível de proteção dos detentores não profissionais e a integridade dos mercados de criptoativos. Permite desenvolver um regime claro e o

tratamento proporcional dos emitentes de criptoativos e dos prestadores de serviços de criptoativos, permitindo assim a igualdade de oportunidades no que respeita à entrada no mercado e ao atual e futuro desenvolvimento dos mercados. Pretende igualmente promover a estabilidade financeira e o bom funcionamento dos sistemas de pagamento, bem como obviar aos riscos que possam advir, para a política monetária, de criptoativos que procuram estabilizar o seu preço em relação a um ativo específico ou a um conjunto de ativos. Pretende preservar a competitividade dos Estados-Membros nos mercados financeiros e tecnológicos internacionais e proporciona aos clientes benefícios significativos em termos de acesso a serviços financeiros e de gestão de ativos mais baratos, mais céleres e mais seguros.

2. O regime da União para os mercados de criptoativos não pretende regulamentar a tecnologia DLT subjacente. Os atos legislativos da União deverão evitar a imposição de encargos regulamentares desnecessários e desproporcionados à utilização de tecnologia, uma vez que a União e os Estados-Membros procuram preservar a sua competitividade no mercado mundial.

6.2.3. Estrutura

1. O Regulamento encontra-se dividido em 9 títulos.

No título primeiro, foi determinado o objeto, o âmbito de aplicação e algumas definições importantes no contexto dos criptoativos. No artigo 1.º, n.º 1, o Regulamento estabelece requisitos uniformes para a oferta pública e a admissão à negociação numa plataforma de negociação de três tipos de criptoativos que iremos explorar de seguida.

O Regulamento estabelece requisitos uniformes no que diz respeito, nomeadamente, a requisitos de transparência e divulgação para emissão e admissão à negociação de criptoativos na alínea a) e em matéria de autorização e supervisão de prestadores de serviços de criptoativos, emitentes de criptofichas referenciadas a ativos e emitentes de criptofichas de moeda eletrónica na alínea b).

2. No artigo 2.º, n.º 1 é estabelecida uma regra, à partida, bastante abrangente, mas que é delimitada nos números seguintes, tanto de forma objetiva como subjetiva. Este Regulamento aplica-se a todas as pessoas singulares e coletivas e a outras empresas envolvidas na emissão, oferta pública e a admissão à negociação de criptoativos, entre outros aspetos.

Por exemplo, nem todos os criptoativos entram no âmbito objetivo do Regulamento, estando excluídos nomeadamente criptoativos já definidos como instrumentos financeiros nos termos da DMIF II – alínea a) do artigo 2.º, n.º 2.

Os atos legislativos da União em matéria de serviços financeiros deverão nortear-se pelo princípio *"mesma atividade, mesmo risco, mesmas regras"* e pelo princípio da neutralidade tecnológica. Por isso, os criptoativos abrangidos pelos atos legislativos da União já em vigor em matéria de serviços financeiros deverão continuar a ser regulados pelo quadro regulamentar em vigor e não pelo Regulamento em análise. De facto, alguns criptoativos são equiparáveis a instrumentos financeiros na aceção do artigo 4.º, n.º 1 ponto 15 da DMIF II, contudo a maioria desses criptoativos não é abrangida pelo âmbito de aplicação da legislação da União em matéria de serviços financeiros.

O Regulamento não se aplica também a criptoativos únicos e infungíveis com outros criptoativos – os tão famosos *NFTs*. Para que o criptoativo seja considerado único e não fungível, os ativos ou os direitos representados também deverão ser únicos e não fungíveis. A exclusão dos criptoativos únicos e não fungíveis do âmbito de aplicação do Regulamento não prejudica a classificação dos mesmos como instrumentos financeiros. O Regulamento aplica-se a criptoativos que, embora pareçam ser únicos e não fungíveis, tenham características efetivas ou associadas à sua utilização que fazem com que sejam de facto fungíveis e não únicos.

Os criptoativos emitidos por bancos centrais na qualidade de autoridade monetária ou por outras entidades públicas não devem estar sujeitos ao quadro da União que abrange os criptoativos, assim como não o devem estar os serviços relacionados com este tipo de criptoativos. Os serviços conexos que são prestados por esses bancos centrais que atuam na qualidade de autoridade monetária ou por outras autoridades públicas também não

deverão estar sujeitos a esse regime. Tendo em conta o ambiente descentralizado em que os criptoativos existem e são transacionados, esta solução parece-nos adequada.

3. No artigo 3.º, n.º 1 são apresentadas algumas definições importantes nomeadamente a definição de criptoativo no n.º 5: *"uma representação digital de valor ou de direitos que pode ser transferida e armazenada eletronicamente, recorrendo à tecnologia de registo distribuído ou a outra tecnologia semelhante"*. Sem prejuízo das limitações que vimos anteriormente.

Os criptoativos são uma das principais aplicações das DLT. Os criptoativos são representações digitais de valores ou de direitos suscetíveis de trazer benefícios significativos aos intervenientes no mercado, nomeadamente aos detentores não profissionais de criptoativos. As representações de valores incluem o valor externo, não intrínseco, atribuído a um criptoativo pelas partes interessadas ou pelos intervenientes no mercado, o que significa que o valor é subjetivo, baseando-se apenas nos interesses do comprador do criptoativos.

Este Regulamento define três categorias de criptoativos:

- Criptofichas referenciadas a ativos que visam estabilizar o seu valor por referência a outro valor ou direito, ou a uma combinação de ambos, incluindo uma ou várias moedas oficiais;
- Criptofichas de moeda eletrónica que funcionam como substitutos eletrónicos de moedas e notas, sendo usadas maioritariamente para pagamentos;
- Outras que não se insiram nem na categoria de criptofichas referenciadas a ativos nem criptofichas de moeda eletrónica nomeadamente as criptofichas de consumo.

Estas categorias não correspondem à tripartição clássica de *tokens* monetários, de utilização e de investimento. Os *tokens* referenciados a ativos e de moeda eletrónica corresponderão, normalmente, a um subgrupo de *tokens* monetários conhecidos como *stablecoins*, ou seja, criptoativos cujo valor é determinado por referência a um ou mais ativos reais subjacentes tais como moedas com curso legal ou matérias-primas[19].

[19] ANTÓNIO GARCIA ROLO, *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, revista n.º 18/2022 CIDP, disponível em https://ssrn.com/abstract=4123583, 2022, pp. 12 e 13.

Esta distinção justifica-se tendo em conta a necessidade de estabelecer um regime mais brando para as criptofichas não referenciadas a ativos e que não sejam de moeda eletrónica e, por oposição, um regime mais exigente para as *stablecoins*. Esta maior exigência do regime aplicável às *stablecoins* tem como justificação um conjunto de preocupações de índole prudencial como os efeitos das *stablecoins* na estabilidade financeira e comportamental nomeadamente a proteção dos investidores e detentores destas moedas.

Para assegurar que todas as ofertas públicas de criptoativos que não sejam criptofichas referenciadas a ativos ou criptofichas de moeda eletrónica na União, tal como todas as admissões de tais criptoativos à negociação numa plataforma de negociação, são devidamente monitorizadas e supervisionadas pelas autoridades competentes, todos os emitentes de criptoativos devem ser pessoas jurídicas.

4. No título segundo regula as ofertas e a comercialização, junto do público, de criptoativos que não sejam criptofichas referenciadas a ativos nem criptofichas de moeda eletrónica. Todas as ofertas públicas deste tipo de criptoativos e admissões de criptoativos à negociação numa plataforma de negociação devem ser devidamente acompanhadas e supervisionadas pelas autoridades competentes. Todos os oferentes e pessoas que solicitam a admissão à negociação devem ser pessoa coletivas. O artigo 5.º determina os requisitos necessários para a admissão deste tipo de criptofichas à negociação.

O emitente deste tipo de criptoativos deve cumprir todos os requisitos do artigo 4.º, sendo um destes requisitos a obrigação de elaborar um *white paper* sobre o criptoativo em causa em conformidade com o artigo 6.º e com o anexo I. Após a publicação do *white paper*, o emitente dos criptoativos pode oferecer estes na União ou solicitar a sua admissão numa plataforma de negociação. Este *white paper* pretende promover a transparência que tanto se procura com a aprovação deste Regulamento.

Poderia haver margem para qualificar este livro como tendo a natureza de prospeto, contudo o Regulamento desmente esta afirmação na alínea d) do artigo 18.º, n.º 6. Este deve conter informações gerais sobre o emitente, o projeto a realizar com o capital mobilizado, a oferta pública de criptoativos ou a sua admissão à negociação numa plataforma desse género, os direitos e obrigações inerentes aos criptoativos, a tecnologia subjacente utilizada para esses ativos e os riscos conexos. Os requisitos de elaboração e publicação do

white paper não se aplicam a ofertas de criptoativos se estas forem efetuadas a menos de 150 pessoas por Estado-Membro ou se se destinem apenas a investidores qualificados e nos casos em que os criptoativos só possam ser detidos por esses investidores qualificados. Também as ofertas que, num período de 12 meses, não excedam os 10.000.00 euros ficam isentas da obrigatoriedade de elaboração de um *white paper*.

O artigo 13.º prevê um direito de resolução a que se chama direito de retratação, nos termos do qual os emitentes devem conceder, a qualquer detentor não profissional que compre criptoativos diretamente a um oferente ou ao prestador de serviços de criptoativos que coloque os criptoativos em nome desse oferente e que os subscreva no prazo de 14 dias corridos, a possibilidade de exercer o direito de retratação sem custos e sem fundamento. O direito de retratação não deve ser aplicável quando os criptoativos que não sejam criptofichas referenciadas a ativos ou criptofichas de moeda eletrónica são admitidos à negociação numa plataforma deste género, uma vez que o preço desses criptoativos dependerá das flutuações do mercado de criptoativos.

O artigo 15.º estabelece uma fonte de responsabilidade pelas informações prestadas no *white paper* do criptoativo.

5. No título terceiro, são reguladas especificamente as criptofichas referenciadas a ativos.

De acordo com o artigo 3.º, n.º 1 ponto 6, uma criptoficha referenciada a ativos é um tipo de criptoativo que procura manter um valor estável tendo como referência o valor de várias moedas fiduciárias com curso legal, uma ou várias mercadorias, um ou vários criptoativos ou uma combinação desses tipos de ativos. Estas visam frequentemente a sua utilização como meio de pagamento para adquirir bens e serviços ou como reserva de valor. Tal acarreta riscos mais significativos em matéria de proteção do consumidor e de integridade do mercado do que outros criptoativos.

As chamadas criptomoedas estáveis algorítmicas, ou seja, as criptomoedas que procuram manter um valor estável por meio de protocolos que preveem o aumento ou diminuição

da oferta de tais criptoativos em função das alterações na procura, não devem ser consideradas criptofichas referenciadas a ativos. Essa classificação só faria sentido se estas não procurassem estabilizar o seu valor por referência a um ou vários outros ativos.

No primeiro capítulo descreve o procedimento de autorização dos emitentes de criptofichas referenciadas a ativos, bem como a aprovação do *white paper* pelas autoridades nacionais competentes – artigos 16.º a 19.º, anexos I e II.

As instituições de crédito autorizadas ao abrigo da Diretiva 2013/36/UE não deverão necessitar de outra autorização ao abrigo deste Regulamento para oferecer ou solicitar a admissão à negociação de criptofichas referenciadas a ativos. Deverão aplicar-se os procedimentos estabelecidos na Diretiva indicada, que devem ser completados pela obrigação de notificar a autoridade competente do Estado de origem, dos elementos que permitam à autoridade em causa verificar a capacidade de o emitente oferecer ou solicitar a admissão à negociação destas criptofichas – artigo 17.º.

O artigo 18.º regula precisamente o conteúdo do pedido de autorização que terá de ser feito pelas pessoas coletivas ou outras empresas que pretendem fazer uma oferta pública ou solicitar a admissão à negociação deste tipo de criptofichas. Os emitentes deste tipo de criptofichas devem, em qualquer circunstância, fornecer aos detentores dessas criptofichas informações claras e corretas.

O *white paper* deve incluir informações sobre o mecanismo de estabilização, a política de investimento dos ativos de reserva, os mecanismos de custódia desses ativos e os direitos conferidos aos detentores. Quando os emitentes não confiram créditos ou direitos de resgate diretos sobre os ativos de reserva a todos os detentores de tais criptofichas, o *white paper* deve conter uma advertência clara nesse sentido, bem como as comunicações comerciais deste emitente. Qualquer evento passível de ter um impacto significativo no valor das criptofichas ou dos ativos de reserva deve ser divulgado, independentemente desses criptoativos serem ou não admitidos a negociação.

Para estarem autorizados a operar na União, os emitentes de criptofichas referenciadas a ativos têm de estar constituídos como entidade jurídica estabelecida na União – artigo 15.º. Se tal não se verificar e se não tiver sido publicado o *white paper*, o emitente não

poderá oferecer ao público criptofichas referenciadas a ativos, nem podem estas ser admitidas à negociação numa plataforma de negociação.

O artigo 22.º regula a comunicação de informação sobre criptofichas referenciadas a ativos e o artigo 26.º estabelece a responsabilidade dos emitentes.

No segundo capítulo estabelece as obrigações dos emitentes de criptofichas referenciadas a ativos. Refere nomeadamente que estes devem atuar com honestidade, equidade e profissionalismo – artigo 27.º. O artigo 32.º trata de identificação, prevenção, gestão e divulgação de conflitos de interesses.

O terceiro capítulo diz respeito a reserva de ativos – artigo 36.º. Existe uma obrigação de constituição e manutenção, por parte dos emitentes de criptofichas referenciadas a ativos, a todo o momento, de uma reserva de ativos. De forma a proteger os detentores deste tipo de criptofichas face a uma diminuição do valor dos ativos que garantem o valor das ditas criptofichas, os emitentes destas criptofichas devem investir os ativos de reserva em ativos seguros e de baixo risco – artigo 38.º. Caso o valor das criptofichas referenciadas a ativos varie significativamente face ao valor dos ativos de reserva, os detentores dessas criptofichas devem ter o direito de solicitar diretamente ao emitente o resgate das suas criptofichas contra ativos de reserva.

O quarto capítulo estabelece regras para a aquisição de emitentes de criptofichas referenciadas a ativos.

O quinto capítulo, no artigo 43.º, estabelece os critérios necessários para determinar se uma criptoficha referenciada a ativos é significativa. Para tal, é necessário que estejam preenchidos os critérios mencionados no n.º 1 deste artigo. Podem ser consideradas significativas, nomeadamente tendo em conta a considerável base de potenciais clientes dos seus promotores e acionistas e a sua potencial capitalização de mercado elevada. As criptofichas referenciadas a ativos com natureza significativa, por serem passíveis de ser utilizadas por um elevado número de detentores e suscitarem particulares desafios em matéria de estabilidade financeira, transmissão da política monetária ou soberania monetária, devem estar sujeitas a requisitos mais rigorosos do que as demais criptofichas referenciadas a ativos.

Contudo, de acordo com o artigo 44.º, será possível, através de uma autorização, o emitente de uma criptoficha referenciada a ativos qualificar voluntariamente a criptoficha em causa como significativa. Com a classificação de criptoficha significativa, acrescem algumas obrigações nomeadamente uma política de gestão da liquidez – artigo 45.º.

No sexto capítulo são regulados planos de recuperação e de reembolso.

6. No título quarto são reguladas as criptofichas de moeda eletrónica.

De acordo com o artigo 3.º, n.º 1 ponto 7, uma criptoficha de moeda eletrónica é um tipo de criptoativo cujo objetivo principal é ser utilizado como meio de troca e que procura manter um valor estável por referência ao valor de uma moeda fiduciária com curso legal. A função destes criptoativos é muito semelhante à função da moeda eletrónica na aceção do artigo 2.º, ponto 2 da Diretiva 2009/110/CE. À semelhança destas, são considerados substitutos eletrónicos de moedas e notas e são utilizados para fazer pagamentos.

Contudo, existe uma diferença importante entre estas duas realidades que justifica a existência de um regime exigente neste caso. Os detentores das moedas eletrónicas, na aceção do artigo 2.º, dispõem sempre de um crédito sobre a instituição da moeda eletrónica e têm o direito contratual de resgatar a sua moeda eletrónica contra moeda fiduciária com curso legal, ao valor nominal dessa moeda. Já alguns criptoativos que têm por referência uma moeda com curso legal, não conferem aos seus detentores um crédito desse tipo sobre os emitentes dos ativos e podem ficar fora do âmbito de aplicação da Diretiva 2009/110/CE. Outros não conferem um crédito ao valor nominal dessa moeda ou limitam o período de resgate.

No primeiro capítulo, descreve os requisitos para oferta pública ou admissão à negociação de criptofichas de moeda eletrónica – artigo 48.º.

No artigo 51.º e no anexo III, são estabelecidos os requisitos relativos ao *white paper* que acompanha a emissão de criptofichas de moeda eletrónica. Terão de constar deste livro nomeadamente informações sobre os riscos associados ao emitente de criptofichas de moeda eletrónica e à execução de qualquer eventual projeto. Quando a emissão destas criptofichas for inferior a um determinado limiar ou quando as criptofichas só possam ser

detidas exclusivamente por investidores qualificados, os emitentes não devem ser sujeitos aos requisitos de autorização, mas devem sempre elaborar o *white paper* sobre criptoativos e apresentá-lo à respetiva autoridade competente.

O *white paper* deve conter todas as informações relevantes sobre o emitente, sobre a oferta de criptofichas ou a sua admissão à negociação numa plataforma de negociação que sejam necessárias para permitir a potenciais compradores tomar uma decisão informada. Também deve indicar explicitamente que os detentores destas moedas têm direito a resgatar as respetivas criptofichas de moeda eletrónica em moeda fiduciária ao valor nominal a qualquer momento. Por outro lado, os emitentes devem ter a possibilidade de cobrar uma comissão caso os detentores solicitem o regaste das respetivas criptofichas em moeda fiduciária.

No segundo capítulo é estabelecida a classificação destas moedas como significativas nos artigos 56 e seguintes. Estas representam um risco mais elevado para a estabilidade financeira e por isso estão sujeitos a requisitos adicionais como temos visto. Também é possível que o emitente pretenda que a sua criptoficha seja classificada como significativa, ou seja, de forma voluntária – artigo 57.º.

7. Tendo em conta o facto de maioria dos Estado-membros não terem regulamentação relativa à prestação de serviços de criptoativos, foi criado este sistema. A necessidade de criar este sistema surgiu também pelo facto de existirem riscos nesta prestação de serviços que deverão ser acautelados. Temos como objetivos da regulação a proteção de investidores, a integridade do mercado e a estabilidade financeira. O título quinto contém disposições sobre a autorização e condições de funcionamento dos prestadores de serviços de criptoativos.

Os serviços de criptoativos só devem ser prestados por entidades jurídicas com sede social num Estado-Membro em que se exerçam atividades comerciais substanciais, incluindo a prestação de criptoativos. Estes serviços devem também possuir uma autorização para desempenhar a função de prestadores de serviços de criptoativos pela autoridade competente do Estado-Membro onde se situa a referida sede social. O Regulamento não obsta à possibilidade de pessoas estabelecidas na União recorrerem, por iniciativa própria, aos serviços de criptoativos de uma empresa de país terceiro.

Enquanto a escala de prestadores de serviços for reduzida, o poder de autorizar e supervisionar os mesmos deve ser conferido às autoridades nacionais competentes. Os prestadores de serviços devem atuar sempre com honestidade, equidade e profissionalismo e no melhor interesse dos seus clientes.

O primeiro capítulo estabelece disposições sobre a autorização de prestadores de serviços. A ESMA, em estreita cooperação com a EBA, elabora projetos de normas técnicas de execução com vista a desenvolver formulários, modelos e procedimentos normalizados para a informação a incluir no pedido de autorização como prestador de serviços de criptoativos – artigo 62.º, n.º 6.

No segundo capítulo impõe requisitos a todos os prestadores de serviços de criptoativos – artigos 66.º e seguintes. Dentro destes requisitos encontramos a atuação com honestidade, lealdade e profissionalismo, sempre no melhor interesse dos seus clientes. De forma a assegurar a proteção contra os riscos do branqueamento de capitais e financiamento de terrorismo, é necessário também que estes prestadores de serviços controlem de forma reforçada as operações que envolvam clientes ou instituições de países terceiros identificados como países de risco por exemplo. Estabelece requisitos prudenciais adicionais no artigo 67.º: deve ser definido um montante fixo ou proporcional às respetivas despesas gerais fixas do ano anterior, em função dos tipos de serviços que estes indivíduos prestam. Os prestadores de serviços estão sujeitos a requisitos estritos em matéria de governação – artigo 68.º.

Estes devem dispor de mecanismos adequados à salvaguarda dos direitos de propriedade dos clientes sobre os criptoativos que detêm. Quando o seu modelo exija que detenham fundos na aceção do artigo 4.º, ponto 25, da Diretiva (UE) 2015/2366, sob forma de notas de banco e moedas, moeda escritural ou moeda eletrónica pertencente aos respetivos clientes, os prestadores de serviços devem proceder à colocação desses fundos junto de uma instituição de crédito ou um banco central. Estes só devem ser autorizados a efetuar transações de pagamento se estiverem autorizados como instituições de pagamento, na aceção da Diretiva (UE) 2015/2366.

No terceiro capítulo estabelece os requisitos aplicáveis a serviços específicos como plataformas de negociação de criptoativos – artigo 76.º. Estes últimos devem dispor de regras

de funcionamento pormenorizadas, assegurar que os sistemas e procedimentos sejam suficientemente resilientes e estar sujeitos a um padrão de transparência pré e pós negociação adaptada ao mercado de criptoativos. Os prestadores de serviços devem assegurar que as negociações realizadas na sua plataforma de negociação são liquidadas e registadas com celeridade nas DLT. Devem dispor de uma estrutura de comissões transparente para os serviços prestados, a fim de evitar a colocação de ordens que possam contribuir para o abuso de mercado ou condições de negociação desordenadas.

No quarto capítulo especifica as regras relativas à aquisição de prestadores de serviços de criptoativos – artigos 83.º e seguintes.

No quinto capítulo estão estalecidas regras relativas aos prestadores significativos de serviços de criptoativos – artigos 85.º e seguintes.

8. Cumpre assegurar a confiança dos utilizadores nos mercados de criptoativos e na integridade dos mesmos, por isso o título sexto estipula proibições e requisitos com vista a evitar o abuso de mercado envolvendo criptoativos admitidos à negociação em plataforma de negociação. São estabelecidas regras específicas que proíbem determinados comportamentos que possam minar a confiança dos utilizadores nos mercados de criptoativos e na sua integridade, nomeadamente transações com base em informação privilegiada.

No artigo 87.º, estabelece-se a definição de informação privilegiada ao individualizar os casos em que estamos perante uma informação privilegiada e indica que um emitente cujos criptoativos sejam admitidos à negociação numa plataforma de negociação tem de divulgar a informação privilegiada – artigo 88.º.

9. O título sétimo dá-nos informações pormenorizadas sobre os poderes das autoridades nacionais competentes, da EBA e da ESMA. São conferidos a estas entidades poderes suficientes para supervisionar a emissão de criptoativos bem como as ações dos prestadores de serviços de criptoativos, incluindo o poder de suspender ou proibir uma emissão de criptoativos ou a prestação de um serviço de criptoativos e de investigar infrações às regras relativas ao abuso de mercado. Têm igualmente o poder de impor sanções aos emitentes de criptoativos.

A EBA tem a tarefa de supervisionar os emitentes de criptofichas referenciadas a ativos significativas. Esta deve criar um colégio de supervisores para os emitentes de criptofichas referenciadas a ativos significativas. Os emitentes em causa devem facilitar a cooperação e o intercâmbio de informações entre os seus membros e emitir pareceres não vinculativos sobre as medidas de supervisão ou alterações de autorização. O mesmo para as criptofichas de moeda eletrónica.

Cabe às autoridades competentes responsáveis pela supervisão, nos termos da Diretiva 2009/110/CE, a supervisão dos emitentes de criptofichas de moeda eletrónica. No que toca a criptofichas de moeda eletrónica significativas, é necessária uma dupla supervisão, tanto pelas autoridades competentes como pela EBA.

A ESMA, em estreita colaboração com a EBA, deverá ser incumbida de emitir orientações sobre sistemas e protocolos de segurança, destinados a especificar melhor as normas da União.

O artigo 97.º visa a promoção da convergência em matéria de classificação de criptoativos.

10. O exercício da delegação com vista à adoção de atos delegados da Comissão é abrangido pelo título oitavo. O Regulamento habilita a Comissão a adotar atos delegados que estabeleçam determinados pormenores, requisitos e mecanismos, conforme o disposto no Regulamento – artigo 139.º.

Por fim, o título nono inclui disposições transitórias e finais, incluindo a obrigação de a Comissão apresentar um relatório que avalie o impacto do Regulamento – artigo 140.º.

7. *BLOCKCHAIN*

7.1. Contextualização

1. A tecnologia *blockchain*, que serve de base à *Bitcoin* que iremos explorar já a seguir, é uma tecnologia descentralizada de registo, tratamento e armazenamento eletrónico de dados, sem registo central ou responsável único pelos dados. Esta tem por base uma ideia de distribuição da responsabilidade pelos diversos participantes. Após a realização de uma transação, cabe a todos os utilizadores aprovar a mesma para que esta se possa consolidar na plataforma. Uma vez validados, os registos têm força vinculativa para todos os participantes[20]. Apenas quando é atingido um consenso multilateral é que pode ser introduzida uma nova informação, a qual não pode ser objeto de alteração, salvo se ocorrer novo consenso[21].

2. Com a publicação do artigo redigido por SATOSHI NAKAMOTO, intitulado *"Bitcoin: A Peer-to-Peer Electronic Cash System"*[22], surge o primeiro criptoativo e criptomoeda. Nesta publicação Satoshi Nakamoto desenvolveu a ideia de uma rede *peer-to-peer* que permitisse aos seus utilizadores transferir entre si unidades de *Bitcoin*, tendo por base um sistema descentralizado que não requeresse a intervenção de uma autoridade governamental para emitir unidades de criptomoeda ou verificar as transações dos seus utilizadores[23]. Pretendia-se, para além disso, resolver um problema de dupla alienação através de um servidor que criasse um registo público das transações realizadas, organizado por ordem cronológica[24].

---

[20] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, pp. 3 e 4.
[21] HUGO RAMOS ALVES, "Smart Contracts: Entre a tradição e a inovação", em *Fintech II – Novos Estudos sobre a Tecnologia Financeira*, António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (coord.), Almedina, 2019, p. 202.
[22] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, p.1.
[23] ANTÓNIO GARCIA ROLO, *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, revista nº 18/2022, CIDP, disponível em https://ssrn.com/abstract=412358, 2022. pp. 2 e 3; SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, p. 1.
[24] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, p. 1; USAMAN W. CHOHAN, *A History of Bitcoin*, Notes of the 21st century, disponível em at: https://ssrn.com/abstract=3047875, 2022. p. 8; ELIZA MIK, "Blockchains – A

As unidades de *Bitcoin* foram originalmente utilizadas para o pagamento de bens e serviços, podendo também ser convertidas em moeda com curso legal, não tendo nenhum ativo subjacente e não estando o seu preço dependente do valor de nenhum ativo, mas antes da procura[25].

Pouco depois do surgimento da *Bitcoin*, surgiram mais moedas e, em 2015, foi lançado o sistema *Ethereum* e a respetiva criptomoeda *Ether*, que permitiu aos seus utilizadores criar os seus próprios criptoativos e fez com que a *blockchain* encontrasse outra vocação – servir de tecnologia subjacente aos *smart contracts* dos quais falaremos mais à frente[26].

Na sequência do lançamento do sistema *Ethereum*, o período compreendido entre 2016 e 2018 foi marcado pelo aparecimento, cada vez mais frequente, das ofertas públicas de moeda ou *Initial Coin Offerings* (ICOs), nas quais vários operadores criavam uma criptomoeda que seria subscrita por investidores que pagariam em moeda com curso legal ou com outras criptomoedas[27]. Nessa fase, as criptomoedas começaram a ir para além das suas funções monetárias originárias. Algumas começaram a oferecer acesso a funcionalidades em determinadas aplicações ou acesso a um dado produto, outras a atribuir ao titular o direito a receber um *cash flow* gerado por um ativo subjacente[28].

Atualmente, existem centenas de *blockchains*, que podem variar em todo o tipo de aspetos, e por isso será mais apropriado falar em DLTs. Este termo permite abranger inúmeras bases de dados sincronizadas e geograficamente dispersas[29].

Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 162.

[25] ANTÓNIO GARCIA ROLO, *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, revista nº 18/2022, CIDP, disponível em https://ssrn.com/abstract=412358, 2022, p. 3; SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, p. 1.; SKATTEVERKET -v- DAVID HEDQVIST, Tribunal de Justiça da União Europeia, processo C 264/14, 22 de outubro de 2015, disponível em http://curia.europa.eu/.

[26] ANTÓNIO GARCIA ROLO, *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, revista nº 18/2022, CIDP, disponível em https://ssrn.com/abstract=412358, 2022, p. 5.

[27] *Idem*, p. 6.

[28] ANTÓNIO GARCIA ROLO, *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, revista nº 18/2022, CIDP, disponível em https://ssrn.com/abstract=412358, 2022, pp. 6 e 7; ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 162.

[29] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 162.

7.2. Características

1. Como vimos anteriormente, a *blockchain* pode ser descrita como uma base de dados distribuída e imutável, gerida de forma descentralizada e, geralmente, de forma autónoma, com verificação algorítmica e criptográfica associada[30].

Antes do surgimento da tecnologia *blockchain*, não era possível coordenar atividades realizadas na *Internet* sem a intervenção de um terceiro elemento imparcial. Com a criação deste sistema, esse problema foi eliminado através da passagem da informação por uma rede de computadores a fim de a tornar mais transparente. A passagem por todos os computadores da rede permite cumprir este objetivo através da resolução de problemas matemáticos que requerem um forte poder computacional para solucionar. Os protocolos da *blockchain* validam as transações feitas na plataforma e garantem que estas nunca são gravadas no repositório de informação mais do que uma vez[31]. Mais à frente analisaremos com mais profundidade estes protocolos.

A *blockchain* é uma base de dados que organiza os dados armazenados por uma rede de computadores. Cada rede está encriptada e organizada em pequenos grupos de informações denominados *blocks* ou blocos. Cada bloco contém informação sobre um conjunto de transações, informações sobre o bloco anterior e também a resposta aos já mencionados problemas matemáticos complexos, utilizados para validar os dados associados ao respetivo bloco. Uma cópia da *blockchain* encontra-se em cada um dos computadores

[30] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 31; AARON WRIGHT / PRIMAVERA DE FILIPPI, *Decentralized blockchain technology and the rise of Lex Cryptographia*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 2015, p. 2; MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 308.

[31] AARON WRIGHT / PRIMAVERA DE FILIPPI, *Decentralized blockchain technology and the rise of Lex Cryptographia*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 2015, pp. 5 e 6; MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://ssrn.com/abstract=2662660, p. 3; MAHER MALHARBY / AAD VAN MOORSEL, *Blockchain-based Smart Contracts: a Systematic Mapping Study*, p. 126.

ligados à rede e esses computadores sincronizam periodicamente para garantir que todos têm acesso a uma base de dados idêntica[32].

Os participantes das redes são designados de *nodes* ou nós. De acordo com o artigo 3.º, n.º 1, ponto 4 do Regulamento MiCA, um nó de rede DLT é um *"dispositivo ou processo que faz parte de uma rede e que detém uma réplica total ou parcial dos registos de todas as transações num registo distribuído"*. Cada nó possui uma identificação que o diferencia dos demais e estes funcionam como terminais de comunicação para quem queira interagir com a *blockchain*[33].

2. Assim, podemos identificar como características principais da *blockchain* a descentralização, anonimato, verificabilidade e a imutabilidade. Vamos densificar cada uma delas de seguida.

7.2.1. Descentralização

1. A tecnologia *blockchain* assenta num consenso descentralizado que permite a transmissão de dados sem a intervenção de um terceiro partido imparcial[34]. Um dos objetivos de todas as redes de *blockchain* é, por isso, ser um sistema de dados onde os seus utilizadores se podem juntar para recolher e armazenar informação sem que exista um ponto de controlo a ditar o modo de funcionamento da rede[35].

---

[32] AARON WRIGHT / PRIMAVERA DE FILIPPI, *Decentralized blockchain technology and the rise of Lex Cryptographia*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 2015, pp. 6 e 7.

[33] ANDREEA BABICEAN, *Blockchain e regulação: perspetivas de uma regulação de valores mobiliários sob a forma de criptoativos*, Almedina, 2024, pp. 20-21.

[34] LIN WILLIAM CONG / ZHIGUO HE, *Blockchain Disruption and Smart Contracts*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764, 2018, revisto em 2020, pp. 1 a 5.

[35] BHARAT BHUSHAN / SAHIL GUPTA / SHUBHAM SINHA, *Emergence of Blockchain Technology: Fundamentals, Working and its Various Implementations*, International Conference on Innovative Computing and Communication, disponível em https://ssrn.com/abstract=3569577, p. 1; LIN WILLIAM CONG / ZHIGUO HE, *Blockchain Disruption and Smart Contracts*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764, 2018, revisto em 2020, pp. 6 e 7.

Assim, os dados de uma *blockchain* não são armazenados num ponto central, mas sim num registo global descentralizado, e quando uma transferência de dados é realizada, esta é imediatamente publicada nesse registo global, atravessando milhões de computadores[36].

Deste modo, como uma *blockchain* é replicada por todos os participantes, suscita-se o problema de sincronizar uniformemente as versões em cada computador. Para tal, foram encontrados mecanismos para permitir o acordo de todos os participantes relativamente à versão correta de dados e a minimização da possibilidade de imposição de uma versão alterada por um dos participantes[37]. É importante referir que este consenso não significa consenso nas decisões individuais de cada nó no que diz respeito, por exemplo, à determinação de que utilizadores ou transações devem ser excluídos ou aceites. O consenso está intimamente ligado àquilo que é determinado pelo algoritmo e nada mais para além disso[38].

2. O consenso pode ser alcançado através de diversos métodos de voto. O Regulamento MiCA, no seu artigo 3.º, n.º 1, ponto 3, define "mecanismo de consenso" como sendo *"as regras e procedimentos através dos quais se chega a um acordo, entre nós da rede DLT, em como uma transação é válida"*.

O mais comum destes mecanismos é o método *Proof-of-Work* que irá depender da resolução de problemas matemáticos complexos por um número de computadores na rede enquanto outros verificam se a solução desses problemas corresponde à transação anterior. Para além deste método de voto, existe outro intitulado *Proof-of-Stake* que irá depender do número de recursos que cada computador na rede detém[39].

---

[36] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 33.
[37] *Ibidem*.
[38] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 166.
[39] AARON WRIGHT E PRIMAVERA DE FILIPPI, *Decentralized blockchain technology and the rise of Lex Cryptographia*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 2015, p. 7.

Podemos assim dizer que o método *Proof-of-Work* diz respeito à demonstração de realização de esforço e o método *Proof-of-Stake* à demonstração de participação ou interesse[40]:

- No primeiro mecanismo, os nós da rede verificam se as informações foram replicadas de transações anteriores e verificam a validade das assinaturas digitais;
- No segundo mecanismo, os titulares de *full* e *master nodes* [41] têm de provar que têm um número de criptoativos determinado por rede para poderem, por um lado, registar novos blocos e, por outro, ser remunerados com novos criptoativos e através de taxas de transação[42].

Como desvantagem, o primeiro tipo de protocolos é lento, demorando um tempo considerável a confirmar a validade de um pagamento. Tal torna-se intolerável com o crescimento exponencial do mercado de criptoativos[43]. Ambos os métodos apresentam como principal desvantagem o seu valor avultado[44].

3. A doutrina faz uma importante distinção, relevante em matéria de descentralização, entre *permissioned blochchains* ou *blockchains* privadas e *permissionless blockchains* ou *blockchains* públicas.

Devido aos problemas associados ao consenso em redes descentralizadas e abertas, têm surgido *blockchains* mais controláveis e previsíveis denominadas *permissioned blockchains*, por oposição às *permissionless blockchains*. Nas *permissioned blockchains*, os utilizadores deverão preencher um conjunto de requisitos para pertencerem à rede. O

[40] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021. p. 36; MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://ssrn.com/abstract=2662660, p. 4.
[41] *Full nodes* são *nodes* completos da rede que permitem ao seu detentor validar as transações da rede por poderem verificar se as informações de uma nova transação já foram utilizadas numa qualquer transação anterior. Os *master nodes*, para além de terem todas as funcionalidades das *full nodes* têm também direitos especiais de voto cf. JOÃO VIERA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021. p. 36.
[42] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021. p. 37.
[43] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016. p. 18.
[44] *Ibidem*.

preenchimento destes requisitos resulta da necessidade de controlar quem são os participantes, quais são os participantes que têm acesso às transações feitas na rede e com a própria realização de transações. Nestas redes é conhecida a identidade dos participantes pelo que estes poderão ser responsabilizados[45]. Como este tipo de *blockchains* não precisa de mecanismos de consenso para funcionar, conseguem ser muito mais rápidas do que as *permissionless blockchains* [46]. Esta consequência deriva do facto de existir uma hierarquia entre os nós, não sendo necessário obter o consentimento de todos os utilizadores para realizar certas operações. Tendo em conta estas restrições, estas *blockchains* podem ter mais privacidade e confidencialidade [47] . Nas *permissionless blockchains* ou *blockchains* públicas, como a *Bitcoin* e a *Ethereum*, o acesso é público, não existindo a necessidade de revelar a identidade, e a gestão da rede é efetuada através de mecanismos de consenso[48]. As *permissionless blockchains* normalmente envolvem um criptoativo nativo que constitui um incentivo à manutenção da plataforma. A manutenção do anonimato nesta sede tem como justificação o facto da confiança se encontrar no código da *blockchain* em si e não nos seus participantes[49].

4. A criação de *permissioned blockchains* parece-nos, em certa medida, uma aproximação a um modelo centralizado, algo que é contrário à essência deste tipo de tecnologias. Nas *permissionless blockchains*, como não existe uma entidade que tenha controlo sobre o mercado, não há nenhuma entidade que possa ser responsável por ele: a confiança reside no código[50]. Essa será a maior vantagem deste modelo de *blockchain*.

---

[45] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em The Cambridge Handbook of Smart Contracts, *Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 164.
[46] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 34.
[47] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em The Cambridge Handbook of Smart Contracts, *Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 163.
[48] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, pp. 34 e 35; LIN WILLIAM CONG / ZHIGUO HE, *Blockchain Disruption and Smart Contracts*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764, 2023. p. 2.
[49] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 162.
[50] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 34.

Por um lado, as *blockchains* públicas permitem o envolvimento de todos os seus utilizadores na regularização dos registos, com base num consenso, e deposita a confiança no próprio código. Por outro lado, as *blockchains* privadas permitem identificar as partes e consequentemente responsabilizá-las na eventualidade de algum problema. A confiança no código será, assim, uma vantagem até ao momento em que ocorra algum problema em sede contratual, mas nessa instância já não haverá possibilidade de travar a execução do contrato e atenuar as suas consequências.

7.2.2. Anonimato

1. O anonimato manifesta-se na encriptação dos elementos identificativos dos indivíduos envolvidos na transação de criptoativos. Existem dois tipos de chaves criptográficas: a chave privada que permite aos utilizadores aceder à sua propriedade criptográfica e permite o controlo das suas contas e a chave pública, cuja função é autenticar o titular e identificar a sua oferta na rede[51]. Apesar de cada chave pública estar ligada a uma morada digital, sendo a transmissão de criptoativos a transação de moedas de uma morada para outra, estas nunca estão ligadas a uma entidade identificável fora do mundo digital[52]. Ou seja, é possível, como é possível no contexto de transações tradicionais, realizar este tipo de transações sem ter acesso à identidade do outro interveniente[53]. Conhecemos já as diferenças entre *permissioned* e *permissionless blockchains* neste ponto.

[51] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 5.
[52] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016, p. 4.
[53] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016, p. 4; ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 26 e 27.

Mais especificamente, a chave pública contém informação relativa à origem e valor de criptoativos em determinada carteira e a chave privada serve apenas para permitir o acesso aos criptoativos associados a essa chave pública[54].

Exemplificando, o A decide enviar *Bitcoin* para a carteira de B, a transação é assinada pela chave privada de A, a transação é enviada pela rede para que possa ser anexada a um bloco, a rede verifica a transação utilizando a chave pública da A e, por fim, a *Bitcoin* é enviada para B que pode ter acesso à mesma através da sua chave privada[55].

2. Apesar de não ser possível identificar a quem pertence certa carteira, podemos afirmar que a mera existência de uma base de dados pública que regista todas as transações feitas na mesma pode ser problemática do ponto de vista da privacidade. Para combater este problema, têm vindo a ser desenvolvidos protocolos que permitem ao utilizador depositar fundos num protocolo, utilizando uma morada, e mais tarde retirá-los do mesmo, utilizando outra morada[56].

Historicamente, as *blockchains* permitem preservar a privacidade dos seus utilizadores por força da pseudonomização: o utilizador não terá de revelar a sua identidade *offline*, será apenas identificado através de uma morada numérica. O *white paper* da *Bitcoin* de SATOSHI NAKAMOTO determinava que "a privacidade será mantida, mantendo as chaves públicas anónimas"[57]. Contudo, alguns consideram este nível de privacidade insuficiente, tendo em conta as novas técnicas de análise e reconhecimento[58].

---

[54] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016. p. 3.
[55] JAZZ OSVALD, *Unjustly enriching the richer: a doctrinal analysis of unjust enrichment and its application to cryptocurrency hard fork and airdrop events*, Australian National University Journal of Law and Technology, 2020, p. 18.
[56] VITALIK BUTERIN / JACOB ILLUM / MATTHIAS NADLER, *et. al*., *Blockchain Privacy and Regulatory Compliance Towards a Practical Equilibrium*, disponível em https://ssrn.com/abstract=4563364 , 2023, p. 1.
[57] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008, p. 6.
[58] VITALIK BUTERIN / JACOB ILLUM / MATTHIAS NADLER, *et. al*., *Blockchain Privacy and Regulatory Compliance Towards a Practical Equilibrium*, disponível em https://ssrn.com/abstract=4563364 , 2023, p. 2.

Por exemplo, *ZK-SNARKs* é uma tecnologia que permite provar reivindicações matemáticas relativas a combinações de dados privados e públicos e satisfaz dois aspetos essenciais:

- *"Zero-knowledge"*: nada sobre os dados privados é revelado, a menos que os dados satisfaçam a reivindicação que se pretende provar.
- *Succinctness*: a prova é curta e pode ser feita rapidamente, mesmo que a reivindicação que se pretende provar envolva computação complexa que demore muito a ser executada[59].

É importante mencionar que, com a implementação deste tipo de protocolos, poderemos ter mais problemas, nomeadamente de utilização destes fundos para operações de branqueamento de capitais ou financiamento de terrorismo, numa perspetiva mais grave, ou para operações de burla. Por isso, estes mecanismos devem ser aplicados com cautela[60].

Por outro lado, a possibilidade de identificação dos nós da rede poderia ter um impacto significativo em situações de mau funcionamento do código ou funcionamento errado do mesmo, para nomear alguns aspetos. Este problema não parece ter resposta no ordenamento europeu, pelo que mais à frente iremos analisar uma forma possível de o resolver no âmbito da modificação, do incumprimento e do enriquecimento sem causa.

3. Devemos ter em conta, por um lado, a importância da característica do anonimato no contexto da tecnologia *blockchain* e, por outro, a necessidade de resolver certas situações prejudiciais para os utilizadores desta tecnologia através da identificação dos mesmos. Quando não haja qualquer problema com o contrato, não há qualquer impedimento a que as partes possam estar anónimas, tendo em conta a possibilidade de duas partes que não se conhecem celebrarem um contrato. Ao invés, quando haja um problema, a identificação dos utilizadores com base nos dados que são disponibilizados ao sistema seria uma forma eficiente de assegurar um julgamento adequado às necessidades dos in-

[59] VITALIK BUTERIN / JACOB ILLUM / MATTHIAS NADLER*, et. al., Blockchain Privacy and Regulatory Compliance Towards a Practical Equilibrium*, disponível em https://ssrn.com/abstract=4563364 , 2023, p. 2.
[60] CHRISTIAN CATALINI / JOSHUA S. GANS, *Some Simple Economics of the Blockchain*, disponível em https://ssrn.com/abstract=2874598, p. 8.

tervenientes. Contudo, tanto a nível de descentralização como de anonimato, não podemos considerar que existam exceções tanto na determinação de um responsável pela ilegalidade como na sua identificação.

O levantamento do anonimato e utilização de técnicas de identificação, tendo por base os elementos fornecidos pelos utilizadores, iriam permitir resolver este problema.

7.2.3. Verificabilidade

1. De forma a assegurar um consenso neste ambiente descentralizado, os protocolos da *blockchain* foram criados para incentivar a recolha de informação responsável e fidedigna, tipicamente num sistema competitivo, de forma a reduzir ao máximo a manipulação de informação[61].

A *blockchain* permite que os participantes verifiquem as transações feitas na rede e executem contratos sem ter de revelar informação sensível a um terceiro elemento. Tal permite assegurar a privacidade dos utilizadores e transações que passam pela rede[62].

A digitalização permitiu que a verificação e os seus custos fossem reduzidos em relação aos custos de verificação fora da rede[63]. A confiança que existia no intermediário financeiro que iria verificar as operações passa para um código e participantes de mercado como já indicámos. Em operações mais complexas, os dados podem também envolver regras e informações necessárias para realizar uma operação específica como seria um *smart contract*. Estes podem ser programados em resposta a novos eventos, o que atribui mais flexibilidade ao processo de verificação. Nos casos em que existam ligações ao mundo *offline*, como seria a situação de recorrência ao oráculo, a verificação a custo zero

[61] LIN WILLIAM CONG / ZHIGUO HE, *Blockchain Disruption and Smart Contracts*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764, 2018, revisto em 2020, p. 7.
[62] CHRISTIAN CATALINI / JOSHUA S. GANS, *Some Simple Economics of the Blockchain*, disponível em https://ssrn.com/abstract=2874598, p. 7.
[63] *Ibidem*.

já é mais difícil e irá depender da concreta ligação entre o elemento *offline* e o seu registo *online*[64].

7.2.4. Imutabilidade

1. De acordo com DEROSE, é a imutabilidade que dá valor intrínseco à *blockchain*, ou seja, esta tem a habilidade de declarar a verdade de forma global independentemente do que qualquer individuo possa fazer para mudar essa verdade[65]. MARC PINKINGTON considera que esta caraterística, ao contrário de outras apresentadas acima, é absolutamente indispensável. Sendo a imutabilidade aquilo que atribui o valor intrínseco aos criptoativos, esta é essencial[66].

A imutabilidade refere-se tanto às transações registadas na *blockchain* como a outros conteúdos nomeadamente o próprio código. A partir do momento em que uma transação é aceite num bloco e esse bloco é registado na rede, já não pode ser alterado. Esta realidade está associada a uma ideia de performance garantida. No que diz respeito ao código, é também impossível alterar o seu algoritmo de consenso[67].

Já outros autores consideram que a imutabilidade apresenta algumas fragilidades. Em certos casos, a reversibilidade é uma qualidade desejada no contexto da *blockchain*. Em primeiro lugar, a possibilidade de conflito entre nós de forma a tentar obter controlo sobre a rede é algo já documentado na economia dos criptoativos. Tal problema poderia ser eliminado através da escolha de intervenientes específicos para fazer validar a informação

[64] CHRISTIAN CATALINI / JOSHUA S. GANS, *Some Simple Economics of the Blockchain*, disponível em https://ssrn.com/abstract=2874598, pp. 9-12.
[65] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016, p. 16.
[66] *Ibidem*.
[67] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 171.

que entra na *blockchain*[68]. Como já vimos, esta barreira pode ser ultrapassada pela utilização de um modelo de *permissioned blockchain*. Em segundo lugar, havendo necessidade de alterar um contrato celebrado entre intervenientes na *blockchain*, apenas a reversibilidade destes sistemas poderia permitir este resultado. Num contexto de imutabilidade, as alterações *ex ante* são impossíveis pois o código irá ser executado como foi programado.

Para contornar a imutabilidade inerente a esta rede e corrigir alguma informação errada que possa ter sido inserida na rede, poderá realizar-se um *hard fork* de forma a criar uma rede com a informação correta. Este representa a cisão na rede por incapacidade de chegar a consenso. Posteriormente, pode existir uma fusão ou junção entre as duas redes, ficando apenas a rede com a informação corrigida a validar as novas transações. Também se poderá contornar essa imutabilidade através da criação de *sidechains* que são *blockchains* que servem de suporte a uma *blockchain* principal, podendo estas primeiras ser alteráveis[69]. Outra hipótese para fugir a esta inflexibilidade pode ser desempenhada no contexto das *permissioned blockchains* pois certos participantes podem editar os conteúdos de um bloco, reverter transações e até alterar o algoritmo[70].

A imutabilidade perde o seu valor a partir do momento em que existe a possibilidade de serem registadas informações erradas que não podem ser alteradas por força da rigidez do sistema[71].

2. Em suma, a imutabilidade tem pontos positivos e negativos, sendo um dos principais pontos positivos a possibilidade de manter um consenso de informação que não possa ser alterado sem critério. Contudo, os pontos negativos parecem sobrepor-se aos positivos. A impossibilidade na modificação de *smart contracts*, assunto que iremos debater em seguida, quando ambas as partes estejam de acordo com a modificação e quando

[68] MARC PINKINGTON, *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660, 2016, p. 19.
[69] JOÃO VIEIRA DOS SANTOS, "Regulação dos Criptoativos" em *Cadernos do Mercado de Valores Mobiliários*, disponível em https://ssrn.com/abstract=3793662, 2021, p. 34.
[70] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 172.
[71] *Idem*, p. 173.

o programa tenha sido redigido de forma contrária ao que as partes pretendiam por exemplo. O facto de não ser possível alterar informações na rede não significa que estas informações sejam necessariamente corretas: existe apenas uma garantia de performance, não de qualidade. Neste momento, a única solução possível será a determinação de regras em matéria de modificação, cessação, etc. de forma a evitar situações em que os contraentes se sintam encurralados pela imutabilidade.

Parece-nos que tanto a vontade dos nós nas tarefas de regularização e uniformização da informação e de implementação de melhores protocolos, por um lado, como a vontade das partes, num contexto contratual, de realizarem determinadas alterações no clausulado, por outro, deverá estar na base da alteração pois são os utilizadores da rede, tanto a nível geral como especial, que são afetados de forma significativa por esta realidade. Vedar a possibilidade de modificação dos contratos e a manutenção da informação independentemente da sua veracidade deviam ser razões suficientes para repensar esta característica.

8. *SMART CONTRACTS* – GENERALIDADES

8.1. Definição de smart contract e os seus desafios

1. Existem várias definições possíveis para aquilo que pode ser considerado um *smart contract*, contudo vamos em primeiro lugar analisar a definição dada pelo criador deste instrumento, Nick Sbazo.

NICK SBAZO definiu o *smart contract* como sendo um *"protocolo de transação computorizado que executa os termos de um contrato"*[72]. Os seus objetivos são principalmente satisfazer condições contratuais, reduzir custos de transação ao assegurar o cumprimento[73] e reduzir a necessidade de intervenção de intermediários externos como instituições bancárias. Podemos apontar como objetivos especificamente económicos a redução de perdas por fraude, custos de cumprimento coercivo menores, entre outros. Presumivelmente, estes poderão tornar o processo de transação completamente transparente e simultaneamente garantir um patamar de privacidade elevado para os seus intervenientes[74].

Existem alguns pontos de consenso na doutrina relativamente à definição de *smart contract,* mas também algumas divergências. Alguns autores exigem que a definição inclua como requisito destes contratos estes habitarem na *blockchain* ou noutra DLT[75]. Outros consideram que estes contratos são independentes da *blockchain* e que a sua qualidade

[72] NICK SBAZO, *Smart Contracts,* disponível em https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, 1994.
[73] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 173.
[74] NICK SBAZO, *Smart Contracts,* disponível em https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, 1994; MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019. p. 756.
[75] RICCARDO DE CARIA, "Definitions of Smart Contracts: Between Law and Code", em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 23.

não depende da validação por via dos protocolos de consenso que asseguram a confiança na *blockchain* em si[76].

Tendo em conta estas ideias, fará agora sentido complementá-las com uma análise mais profunda das termos que compõem a designação: *smart contract*.

Os *smart contracts* podem servir tanto propósitos contratuais como não contratuais, daí o possível problema da designação. Mas nesta sede estamos a falar tanto de contratos criados na rede com linguagem programática como instrumentos contratuais que executam ou complementam contratos tradicionais celebrados *off-chain*[77].

Havendo um conjunto de direitos e obrigações inseridos no clausulado contratual, temos um contrato em sentido técnico. Tendo em conta a liberdade de forma que caracteriza o nosso direito civil, não fará sentido considerar este contrato como uma nova realidade jurídica: é apenas uma nova forma de contratar dentro da moldura legal estabelecida[78]. Mesmo sendo estes *smart contracts* instrumentos de execução ou complemento, estes são considerados elementos de natureza contratual[79].

O termo *smart* refere-se ao grau de complexidade e adaptabilidade dos *smart contracts*[80]. Esses diferentes graus de complexidade permitem fazer uma distinção entre os *shallow smart contracts*, ou seja, os contratos que executam transações simples e os *deep smart contracts* que executam transações complexas[81]. Ao contrário do que possa parecer, este termo não diz respeito ao conceito de IA[82].

---

[76] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 174.
[77] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 22 e 23
[78] *Idem*, p. 25.
[79] *Idem*, p. 26.
[80] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 3.
[81] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 27 e 28.
[82] RICCARDO DE CARIA, "Definitions of Smart Contracts: Between Law and Code", em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019, p. 23.

2. Nick Sbazo propõe, assim, uma definição mais lata de *smart contracts,* apresentada no início deste capítulo. Esta definição é propositadamente lata, tendo em conta as possíveis alterações dos sistemas jurídico e tecnológico. Um *smart contract* é, por isso, um *software*, cujo código liga duas ou mais partes para a execução de um conjunto de efeitos pré-definidos[83].

Do um ponto de vista técnico, um *smart contract* é simplesmente um código informático. Contudo, o seu processo geralmente envolve quatro elementos[84]:

1) *Código*: O código contém todos os detalhes da transação pretendida. A transação pode ser descrita como sendo a transferência de informação em sentido amplo.
2) *Carteira*: A carteira é o espaço digital onde se encontram as chaves criptográficas. Como sabemos, existem dois tipos de chaves criptográficas: a chave privada e a chave pública. A morada desta carteira deriva dos últimos 20 b*ytes* da chave pública.
3) *Arquivo*: O arquivo é o espaço digital onde a transação é armazenada antes de ser registada, o que toma muitas vezes lugar na rede *blockchain*.
4) *Registo*: O registo é onde a transação é definitivamente armazenada. O registo será feito maioritariamente dentro da *blockchain*.

8.2. Tipos de smart contracts

1. A forma e o conteúdo de um *smart contract* pode diferir significativamente com base em três aspetos: o nível de automação no que diz respeito à execução do contrato; o nível de separação entre os termos contratuais e o código que os executa; a discrição e

[83] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 4.
[84] *Idem*, p. 5.

execução pelas partes. Com base nestes aspetos, podemos fazer uma distinção entre dois tipos de *smart contracts*[85].

A primeira categoria diz respeito aos contratos que *apenas* são executados de forma inteligente, podendo ser concluídos dentro ou fora da rede *blockchain*. Mas, mesmo neste primeiro caso, os algoritmos da rede são utilizados exclusivamente como mera ferramenta no processo de formação do contrato[86].

Para o funcionamento destes contratos numa *permissionless blockchain*, a rede cobra uma taxa pelos contratos, que vai aumentar de acordo com a complexidade do contrato. De forma a definir um valor, as *blockchains* têm de recorrer a um oráculo, que permite a conexão à *Internet*.[87] Podemos, assim, concluir que ainda não atingimos uma total autonomia da *blockchain*.

Contudo, com o rápido desenvolvimento dos *smart contracts*, uma nova categoria poderá surgir brevemente: contratos tanto concluídos como executados através da *blockchain*. Ao contrário do que sucede com a primeira categoria de contratos apresentada, a tecnologia *blockchain* pode ser usada para encontrar uma parte contratante e concluir o negócio que depois será executado automaticamente. Os algoritmos não serão apenas uma mera ferramenta, mas também um agente artificial no contexto de formação de um contrato entre dois ou mais agentes[88].

Atualmente, existem apenas *smart contracts* puros, que se desenvolvem totalmente na *blockchain* sem necessidade ou possibilidade de contacto com o mundo *offline* e cuja execução está restringida às informações que constam da *blockchain*, e os *smart contracts* híbridos que incluem oráculos que fazem ligação ao mundo exterior. Quando um elemento do contrato esteja condicionado à sua performance *off-chain*, o *smart contract* deve contactar o oráculo de forma a saber se a performance desse elemento de facto tomou lugar. De forma a transmitir esta informação, os oráculos utilizam a sua chave privada

---

[85] MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019. p. 759.

[86] MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019. p. 760.

[87] *Ibidem*.

[88] *Idem*, pp. 760 e 761.

para assinar caso o evento condicionante tenha de facto ocorrido[89]. Os oráculos colocam em causa a desintermediação e resultam na perda da característica de descentralização[90].

8.3. Vantagens e desvantagens

1. Podemos apontar como vantagens dos *smart contracts* a redução nos custos de transação e litigação, tendo em conta que aquilo que é executado é imutável. A quase inexistente ambiguidade da linguagem programática permite tanto eliminar maior parte dos erros de interpretação como reduzir o tempo deste processo de redação. É importante mencionar que não há uma completa irradicação da possibilidade de erro e, como veremos mais à frente, essa circunstância terá impacto na estrutura tendencialmente imutável onde estes contratos habitam.

Outra vantagem será a possibilidade de assegurar a criação e execução de um contrato sem a intervenção de um terceiro elemento imparcial[91]. Também podemos dizer que, tecnicamente, não há forma de violar estes contratos por força da sua natureza imutável. Contudo, quando a execução é perturbada de qualquer forma, não haverá como assegurar situações de alteração de circunstâncias, a modificação ou cessação do contrato, etc.

Por fim, permite a realização de diversas tarefas tanto contratuais como não contratuais.

2. Por outro lado, os *smart contracts* apresentam um conjunto de vulnerabilidades ao nível da segurança que resultam em perdas financeiras consideráveis. Será possível evitar maior parte destes casos através de uma análise formal dos *smart contracts* antes destes serem colocados na plataforma de *blockchain*[92]. Contudo, esta análise implicaria a

---

[89] ELIZA MIK, "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts,* Blockchain Technology and Digital Platforms, disponível em https://doi.org/10.1017/9781108592239, 2019, pp. 175 e 176.
[90] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 29 e 30.
[91] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 306.
[92] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al*., *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2906.

previsão de todas as circunstâncias que poderão afetar o contrato e, como sabemos por experiência com contratos tradicionais, essa previsão é quase impossível de efetivar. Mas ao contrário do que sucede com os contratos tradicionais, não há forma de remediar possíveis problemas a partir do momento em que se dá início à execução.

No processo anterior à execução na plataforma, são apresentadas várias soluções para resolver este problema nomeadamente as soluções focadas na programação. Tendo em conta que na base de um *smart contract* encontra-se a linguagem na qual é executado, programar estes contratos de forma correta será uma forma de combater as vulnerabilidades apresentadas. Uma das formas de garantir uma programação correta destes contratos poderá passar pela criação de novas linguagens de programação, mas tal ainda não foi plenamente comprovado[93]. Atualmente, a única forma de garantir este resultado será através da escolha de *coders* especializados, o que, mesmo assim, não elimina a possibilidade de erro.

Existem também as soluções focadas na verificação formal. Tipicamente, o teste formal serve para garantir que um *software* se comporta da forma esperada. Isso significa que esta verificação só consegue analisar se um *smart contract* está a ser executado de acordo com as suas especificações, não permite detetar as suas vulnerabilidades a nível material. Assim, a verificação formal automática é apenas uma forma de detetar *bugs* e outros erros técnicos, garantindo o funcionamento correto dos *smart contracts* com base no seu código. Estas ferramentas de verificação formal estão também numa fase experimental ainda[94]. Atualmente, a solução passará novamente para contratação de *coders* especializados para minimizar a possibilidade de erro.

[93] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al*., *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2906.

[94] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al*., *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2906; BHARAT BHUSHAN / SAHIL GUPTA / SHUBHAM SINHA, *Emergence of Blockchain Technology: Fundamentals, Working and its Various Implementations*, International Conference on Innovative Computing and Communication, 2020, p. 3.

Por fim, temos soluções viradas para a otimização. Dentro deste tipo de soluções existem soluções ligadas à otimização da performance ou à otimização da segurança[95].

A performance de um *smart contract* pode ser definida pela velocidade com que os sistemas que regulam este tipo de contratos oferecem respostas, permitindo que o número dos contratos aumente sem comprometer o tempo de resposta. Para ultrapassar dificuldades de performance, os especialistas têm proposto soluções para executar os contratos em paralelo em vez de sequencialmente[96].

A segurança pode ser analisada com base na robustez do sistema no combate contra os ataques internos ou externos. Dentro deste tipo de soluções, temos soluções para detetar vulnerabilidades, modelos de transação privados e soluções ligadas ao fornecimento de dados seguro[97].

Descobrir vulnerabilidades na execução deste tipo de contratos é importante para aumentar a segurança e credibilidade dos *smart contracts*. Para diluir estas vulnerabilidades, têm sido aplicadas várias soluções de análise do clausulado. Como já determinámos, não basta uma verificação formal pois o que irá prevenir situações de ilegalidade será a verificação material[98].

O problema da privacidade representa um grande desafio para os *smart contracts* como já vimos. Apresenta dificuldades no que diz respeito à manutenção de certas funções críticas e as próprias informações em segredo. Numa tentativa para resolver esta questão, KOSBA *et. al*. propuseram o *Hawk*, uma ferramenta que permite aos programadores destes contratos desenvolverem contratos que mantenham a privacidade das partes sem que seja necessário implementar qualquer criptografia extra[99]. Também os protocolos de privacidade que vimos em matéria de anonimato podem ser aplicados, com as devidas precauções.

---

[95] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al., Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, pp. 2907 e 2908.
[96] *Idem*, p. 2908.
[97] *Idem*, p. 2909.
[98] *Idem,* p. 2910.
[99] *Ibidem*.

A execução de um *smart contract* pode implicar a integração de alguma informação que se encontra fora da *blockchain*. Por isso, mecanismos de implementação de informação, como os oráculos, são necessários para criar uma ponte entre a *blockchain* e o mundo exterior, se tal for possível. É absolutamente necessário que as informações provenientes destes oráculos sejam da melhor qualidade pois a qualidade dos dados irá determinar a forma como os *smart contracts* são executados[100]. Tal não é garantido tendo em conta que os oráculos são pessoas ou programas criados por pessoas, existindo sempre margem de erro.

O tratamento de dados dentro da *blockchain* surge como forma de garantir que a transação de dados entre as partes é feita de forma transparente. Alguns exemplos de soluções centradas no tratamento de dados dizem respeito à proveniência dos dados, ao acesso e à partilha dos mesmos[101].

A proveniência dos dados diz respeito ao registo histórico dos dados e às suas origens, registo este que controla o armazenamento, acesso e processamento dos dados, a identidade e o propósito daqueles que inserem estes dados. Garantir a existência deste registo de dados com estas características garante a transparência dos mesmos e reforça a sua integridade. Os *smart contracts*, nesta sede, podem ser utilizados para verificar a origem dos dados antes do início do processo de armazenamento[102].

O acesso aos dados é concedido de acordo com os direitos que as partes tenham para realizar certas operações. Os direitos são concedidos através de políticas de controlo do acesso, sendo estas políticas um conjunto de condições que são avaliadas para garantir ou não o acesso sempre que seja recebido um pedido. Para obter políticas descentralizadas, estas devem ser codificadas como código executável e controladas pela rede. Para esse propósito, os *smart contracts* podem ser utilizados para permitir que o processo de avaliação de políticas seja executado de forma descentralizada. A política de controlo do

[100] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al*., *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2910.
[101] *Ibidem*.
[102] *Idem*, p. 2912.

acesso seria representada assim através de um *smart contract* que avaliaria as condições que concedem o acesso e determinaria se essas teriam sido cumpridas[103].

A partilha de dados traduz-se em tornar os dados disponíveis a outras pessoas que não o seu titular se este o autorizar. Por um lado, a partilha conduz à perda do controlo, por outro, a manutenção dos dados no poder do seu titular permite assegurar um forte controlo sobre os dados, com a contrapartida de esses não serem divulgados aos restantes utilizadores. A tecnologia *blockchain* pode ser utilizada nesta sede pois oferece um banco de informações imutável e tem códigos executáveis para autenticar utilizadores e verificar autorizações da mais variada ordem. Por essas razões, podemos assumir que garante a existência de um sistema de partilha de dados seguro e eficiente[104].

Um dos desafios da existência de biliões de dispositivos é a sincronização da informação, mas existem soluções na *blockchain* para assegurar essa sincronização. Especificamente, os *smart contracts* podem ser utilizados para garantir a autenticação, a sincronização e a integridade dos dados dentro de um sistema com estas características[105].

Apesar dos *smart contracts* preencherem muitas das condições relacionadas como tratamento de dados e dispositivos, eles têm algumas desvantagens por força dos princípios que informam a tecnologia *blockchain*. Em primeiro lugar, os dados guardados nos *smart contracts* estão disponíveis publicamente. Pelo que é requerido que se evite colocar chaves privadas em *smart contracts* para permitir que essa informação esteja disponível publicamente sem violar a privacidade dos intervenientes. Para resolver os problemas de transparência relacionados com a *blockchain*, os estudiosos estão a tentar conceber soluções criptograficamente complexas para garantir a segurança dos dados, mantendo simultaneamente os custos da sua formação baixos.

[103] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al., Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2913.
[104] *Ibidem*.
[105] *Ibidem*.

3. Os *smart contracts* poderão contribuir para o desenvolvimento industrial. Assim, teremos contratos que podem exigir a colaboração de vários tipos de entidades. Dentro destas possibilidades de uso dos *smart contracts* temos soluções centradas e não centradas no lucro[106].

Como sabemos, a segurança, a execução em tempo real e a transparência são objetivos essenciais no desenvolvimento de um *smart contract* inserido na *blockchain*, contudo estes mesmos objetivos podem ser um obstáculo para soluções centradas no lucro. Alguns exemplos de soluções centradas em lucro são soluções baseadas em rastreamento, bens digitais e *crowdsourcing*[107].

O rastreamento em tempo real pode reduzir o tempo de espera na confirmação de informação. A utilização de um sistema distribuído pode ajudar a alcançar este objetivo. Assim, os *smart contracts* podem ser utilizados para automatizar transferências de vários tipos de propriedade sobre bens e, assim, tornar os processos livres de intermediários[108].

A imutabilidade característica dos *smart contracts* torna-os bastante apelativos em vários cenários nomeadamente naqueles em que se requer transferências de dinheiro para respeitar certas regras do acordo como serviços financeiros. A falta de centralização do sistema proporciona um maior controlo e acesso por parte dos investidores. Com esse fim, os *smart contracts* são utilizados para realizar pagamentos internacionais sem a intervenção de instituições bancárias[109].

O *crowdsourcing* é uma forma *online* e distribuída de resolução de problemas na qual indivíduos e organizações adquirem bens e serviços de um grupo grande de participantes. O *crowdfunding* tornou-se uma das formas mais populares de *crowdsourcing*. O *crowdfunding* é um processo em que pequenos investimentos e doações, feitos por grupos organizados de pessoas, apoiam o desenvolvimento de novos projetos em troca de produtos grátis ou outro tipo de reconhecimento. O *crowdsourcing* tradicional é baseado num sistema central em que os requerentes postam tarefas num servidor, contudo este modelo

[106] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al, Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2914.
[107] *Ibidem*.
[108] *Ibidem*.
[109] *Ibidem*.

centralizado enfrenta, neste momento, alguns desafios nomeadamente o seu custo elevado e vulnerabilidade a ataques maliciosos. A *blockchain* é considerada uma tecnologia promissora para o funcionamento destes grupos[110].

Avançando para as soluções não centradas no lucro, a tecnologia *blockchain* é fundamental numa área de colaboração entre várias organizações, tendo em conta a desconfiança que existe quando as partes envolvidas não têm conhecimento de como as suas contribuições são gastas ou controladas. Exemplos deste tipo de soluções são sistemas de voluntariado, sistemas para instituições escolares, etc. Os *smart contracts* permitem realizar uma análise da performance dos dados, o que é difícil de falsificar. Apesar dos benefícios da *blockchain* e *smart contracts* na atualização das operações numa variedade de indústrias não centrados no lucro, verificam-se alguns desafios com a adoção destes procedimentos. Alguns destes desafios são questões legais, falta de protocolos e regras, problemas de privacidade, de escala e intolerância ao erro[111].

Tendo em conta a novidade que caracteriza ainda os *smart contracts*, estes ainda apresentam vários desafios nomeadamente legais, de confiança em recursos fora da rede, imutabilidade e problemas dos mecanismos de consenso como temos vindo a relatar[112].

Como sabemos, a imutabilidade é uma importante característica dos *smart contracts*. A partir do momento em que o *smart contract* é emitido e se inicia o processo de execução, o código não pode ser alterado por nenhuma das partes nem por outros membros da *blockchain*. Na eventualidade de algum erro, a imutabilidade previne, em teoria, qualquer tipo de retificação do contrato que possa ser prejudicial para as partes. Havendo uma alteração de circunstâncias, a alteração do contrato é extremamente desafiante. Para resolver este problema, seria necessário introduzir revisões extensivas e possivelmente caras feitas por especialistas antes da emissão do contrato. Para além disso, qualquer um dos utilizadores pode ser *hackeado* ou reportar informação errónea que ficará na *blockchain* de forma imutável[113].

---

[110] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al.*, *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, pp. 2916 e 2917.
[111] *Ibidem*.
[112] *Idem*, pp. 2918 e 2919.
[113] *Idem*, p. 2919.

A escala é outro dos desafios da tecnologia *blockchain*. Este desafio dá origem a outros como congestão da rede, aumento das taxas de comissão e do tempo necessário para confirmar transações. Para resolver este problema, será necessário conduzir uma vasta investigação para aumentar o número de transações por segundo[114].

Os mecanismos de consenso têm um papel importante na manutenção da segurança, escala e descentralização das redes de *blockchain*. Como sabemos, já existem dois mecanismos de consenso: o *Proof-of-Work* e o *Proof-of-Stake*. O desperdício de recursos que resulta da utilização destes métodos leva a que muitas organizações mudem para mecanismos mais baratos e com custo de energia também mais baixo. Novos mecanismos como *Proof-of-Activity* e *Proof-of-Stake* delegado estar a ser testados de forma a melhorar a sua qualidade, sendo ainda prematuros[115].

De forma a resolver estes problemas, foram apresentadas soluções nomeadamente protocolos de segunda camada e soluções de controlo dos contratos. A primeira surge como uma forma de lidar com o problema de escala da *blockchain*. Enquanto a primeira camada é a camada mais profunda da arquitetura da plataforma, a segunda camada é aquela mais à superfície. Esta última refere-se a múltiplos protocolos construídos em cima do sistema *blockchain*. O principal objetivo desta camada é resolver a questão da velocidade das transações e outras dificuldades que ocorrem nas maiores redes de criptoativos. Um exemplo de uma solução de segunda camada, na rede *Bitcoin*, é a *Bitcoin Lightning Network*. Esta tem como objetivo reduzir custos e tempo despendido, passando as pequenas transações para um ambiente seguro fora da rede para que só as maiores transações sejam tratadas dentro da *blockchain*. Graças a esta segunda camada, parte das transações podem ser tratadas fora da rede principal. Enquanto a rede principal garante segurança, esta segunda camada oferece melhores soluções para o problema da escala[116]. Parece-nos que isto implicaria uma cisão na rede *Bitcoin*, neste caso, que não será muito benéfica para o funcionamento de uma rede única e sincronizada.

---

[114] SHAFAQ NAHEED KHAN / FAIZA LOUKIL / CHIRINE GHEDIRA-GUEGAN, *et. al*, *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021, p. 2919.
[115] *Ibidem*.
[116] *Idem*, pp. 2919 e 2920.

4. Assim, como foi dito no início deste capítulo, a utilização de *smart contracts* tem vantagens e desvantagens no que toca aos mais variados aspetos, mas parecem-nos uma ferramenta revolucionária no mundo contratual digital.

8.4. Relevância legal dos smart contracts

1. De forma que possamos responder a esta pergunta teremos de, em primeiro lugar, relembrar a distinção que fizemos há pouco entre os *smart contracts* que têm como função apenas executar contratos tradicionais, contratos que são escritos em linguagem de código numa primeira instância e *smart contracts* que complementam contratos tradicionais, havendo uma parte digital e uma parte analógica neste conjunto[117].

No primeiro caso, temos um instrumento de execução que tem por base um contrato escrito em linguagem natural. No segundo caso, temos um contrato original, escrito em linguagem programática. No terceiro caso, temos um instrumento que acompanha o contrato tradicional, desempenhando uma função de complemento. Em todas estas formas de utilização de *smart contracts*, temos um elemento contratual por natureza, relacionado com um contrato tradicional ou partindo de um clausulado contratual redigido exclusivamente em código programático[118].

Parece-nos que o recurso a uma linguagem programática nestes moldes é apenas um aproveitamento da liberdade de forma que vigora no nosso direito.

2. O escopo de intervenção legal num *smart contract* é mais reduzido, tendo em conta que podem ser evitadas certas situações nomeadamente no que diz respeito ao incumprimento e certas disputas relativamente à interpretação do clausulado[119]. Cabe a nós

---

[117] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 23.
[118] *Idem*, pp. 24-26.
[119] LAWRENCE AKKA / SAM GOODMAN / MATTHEW LAVY *et. al*., *Legal Statement on Cryptoassets and Smart Contracts*, UK Jurisdiction Taskforce, disponível em https://technation.io/about-us/lawtech-panel, 2019. p. 31.

determinar se de facto haverá menos problemas nesta sede. Tecnicamente, o *smart contract* não permite a sua violação pois a sua execução é imutável: a partir do momento em que é iniciada, não há como voltar atrás[120].

Um código não consegue detetar vícios num contrato, a menos que seja instruído para os detetar. O sistema é baseado nas suas próprias normas e vai executar o acordo com base na sua própria estrutura. Se se desejar a aplicação de qualquer medida, esta tem de constar do código antes de se dar início à execução. Como consequência, o registo dos contratos na *blockchain* pode ser problemático. A razão para tal deve-se ao facto de puderem ocorrer discrepâncias entre o código desejado pelas partes e o código que foi efetivamente executado. Para além disso, haverá sempre o risco de a performance ser afetada por acontecimentos externos ao código, nomeadamente uma falha no sistema[121]. Se o contrato é imutável, à partida não há forma de resolver estas situações.

No que diz respeito a circunstâncias externas, podemos dizer que existe outra distinção importante nesta matéria: *dumb smart contracts* e *smart smart contracts*. Estes primeiros são maioria dos *smart contracts* em vigor neste momento e apresentam pouco flexibilidade na medida em que não estão abertos à evolução dos tempos e ao aparecimento de novas circunstâncias externas; vivem apenas dentro da *blockchain,* pelo que circunstâncias exteriores a ela não podem afetar os contratos. Já os segundos são flexíveis neste ponto, tendo em conta que estão ligados a oráculos que os podem informar sobre os mais variados aspetos de forma a mantê-los atualizados[122].

Independentemente desta realidade, um contrato em código que não tenha em conta todas as circunstâncias que o poderão afetar não é menos merecedor da qualificação como contrato, tendo em conta que os próprios contratos tradicionais não preveem todas as circunstâncias que os possam afetar[123].

---

[120] MICHEL CANNARSA / LARRY A. DIMATTEO / CRISTINA PONCIBÒ, "Smart Contracts and Contract Law" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms,* disponível em https://doi.org/10.1017/9781108592239, 2019, p. 10.
[121] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 8.
[122] MICHEL CANNARSA / LARRY A. DIMATTEO / CRISTINA PONCIBÒ, "Smart Contracts and Contract Law" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms,* disponível em https://doi.org/10.1017/9781108592239, 2019, pp. 9 e 10.
[123] *Idem*, p. 11.

3. Tendo em conta este panorama, podemos dizer que o código e, por maioria de razão os *smart contracts*, são legalmente relevantes ao ponto de criarem parâmetros para regular comportamento social, à semelhança de um contrato tradicional, para além de puderem ter uma função de densificação ou execução deste tipo de contratos. É importante ressalvar também que a qualificação enquanto instrumento contratual dependerá da vontade das partes em atribuir uma natureza contratual a estes instrumentos.

O desafio reside em criar permeabilidade entre o sistema informático e o sistema legal e construir pontes entre eles para que o código utilizado em cada *smart contract* respeite a lei[124]. Alguns pioneiros da *blockchain* e dos *smart contracts* consideram que a *blockchain* não precisa de qualquer regulação pois tecnicamente regula-se pelo seu próprio protocolo[125]. Consideramos que desde que a materialidade das situações que se pretende regular através do *smart contract* coincida com os parâmetros legais aplicáveis e as partes o desejem, podemos defender que os *smart contracts* podem ser vistos como verdadeiros contratos[126]. Não fará sentido rejeitar a qualificação de contrato a um conjunto de direitos e obrigações recíprocas ou à densificação e execução destes conjuntos de informação[127].

Em suma, os *smart contracts* são relevantes legalmente quando as partes o desejem e se verifica uma das funções já indicadas. Quanto à lei aplicável e jurisdição, a resposta ainda é incerta. Vamos explorar esta questão mais à frente.

[124] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, pp. 8 e 9.
[125] *Idem*, p. 9.
[126] *Ibidem*.
[127] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 25.

9. BREVE ENQUADRAMENTO DE DIREITO INTERNACIONAL PRIVADO

1. Na ausência de normas regulamentares ao nível do Regulamento MiCA no que diz respeito a aspetos essenciais do contrato nomeadamente o acordo entre as partes, a capacidade, interpretação, modificação, transmissão, incumprimento e enriquecimento sem causa, teremos de determinar qual o direito a aplicar nestes casos.

2. Temos uma situação privada que precisa de ser regulada, mediante a determinação da ordem jurídica que vai fornecer a disciplina material aplicável[128]. A norma de conflitos competente nesta sede irá determinar qual a ordem jurídica em concreto que o pode fazer.

Em matérias contratuais e extracontratuais, temos de analisar respetivamente os Regulamentos Roma I e Roma II de forma a determinar se os assuntos em causa se enquadram nos âmbitos materiais destes Regulamentos. Caso não sejam enquadráveis de acordo com os critérios estipulados, teremos de recorrer às normas de conflito de direito nacional, neste caso de direito português.

O âmbito de aplicação material do Regulamento Roma I diz respeito a obrigações contratuais em matéria civil e comercial que impliquem um conflito de leis, de acordo com o artigo 1.º, n.º 1 do Regulamento. Não se aplica nenhuma das exceções do n.º 2 do mesmo artigo e por isso podemos avançar com a aplicação deste Regulamento. É importante mencionar que, de acordo com o artigo 2.º, a lei designada pelo Regulamento é aplicável mesmo que não seja a lei de um Estado-membro. Existe liberdade de escolha da lei que regula o contrato de acordo com o artigo 3.º e, na falta de escolha, o artigo 4.º auxilia-nos na determinação da lei a aplicar.

De acordo com o artigo 12.º, a lei aplicável ao contrato por força do Regulamento pode regular nomeadamente a interpretação; o cumprimento das obrigações dele decorrentes; os limites dos poderes atribuídos ao tribunal pela respetiva lei de processo, as consequências do incumprimento total ou parcial dessas obrigações, incluindo a avaliação do dano, na medida em que esta avaliação seja regulada pela lei; as diversas causas de extinção das obrigações e também as consequências das invalidades. O n.º 2 deste artigo diz-nos que,

[128] LUÍS DE LIMA PINHEIRO, *Direito Internacional Privado I – Introdução e Direito de Conflitos, Parte Geral*, 3ª ed. refundida, AAFDL Editora, 2019, p. 227.

no caso de cumprimento defeituoso, deve atender-se à lei do país onde é cumprida a obrigação. No que diz respeito a um possível problema de capacidade, o artigo 13.º diz-nos que, num contrato entre pessoas que se encontram no mesmo país, uma pessoa singular considerada capaz segundo a lei desse país só pode invocar a sua incapacidade que resulte da lei de outro país se, no momento da celebração do contrato, o outro contraente tinha conhecimento dessa incapacidade ou a desconhecia por negligência.

O âmbito de aplicação do Regulamento Roma II diz respeito a obrigações extracontratuais nomeadamente casos de enriquecimento sem causa. O artigo 1.º, n.º 1 diz-nos que este Regulamento se aplica em situações que envolvam um conflito de leis, às obrigações extracontratuais em matéria civil e comercial. Não está preenchida nenhuma das exceções do n.º 1 do mesmo artigo. O artigo 2.º dá-nos uma definição de obrigações extracontratuais para efeitos do Regulamento, dizendo que *"o dano abrange todas as consequências decorrentes da responsabilidade fundada em ato lícito, ilícito ou no risco, do enriquecimento sem causa, da negotiorum gestio ou da culpa in contrahendo"*. Novamente, o artigo 3.º, determina que é aplicável a lei designada pelo presente Regulamento, mesmo que não seja lei de um Estado-membro.

De acordo com o artigo 10.º, nos casos de enriquecimento sem causa, se uma obrigação extracontratual que decorra do enriquecimento sem causa, estiver associada a uma relação existente entre as partes, baseada nomeadamente num contrato ou em responsabilidade de qualquer tipo, que apresente uma conexão estreita com esse enriquecimento sem causa, é aplicável a lei que rege essa relação. Os números seguintes ajudam-nos a determinar a lei aplicável nos casos em que não seja possível determinar por aplicação do n.º 1.

3. Estas são as regras que temos de seguir para identificar o direito a aplicar em determinado caso, cabendo a nós nesta sede determinar as soluções que temos em matéria de direito dos contratos.

10. PROBLEMAS CLÁSSICOS NUMA NOVA REALIDADE: CONTRATOS TRADICIONAIS VS. *SMART CONTRACTS*

10.1. Acordo entre as partes

10.1.1. Proposta e aceitação

1. O negócio jurídico, enquanto manifestação última da eficácia jurídica da natureza humana, assenta em declarações de vontade. Efetivamente, apenas a vontade declarada, isto é, exteriorizada, de modo a puder ser reconhecida pelos operadores jurídicos e pelo próprio sistema, pode provocar efeitos de Direito[129].

A declaração de vontade comporta dois elementos: a vontade humana e a declaração. A vontade pode ser decomposta em três planos: a vontade do comportamento, a vontade da declaração e a vontade do negócio[130]. A vontade do comportamento permite constatar a presença de uma efetiva ação humana. A vontade de declaração implica a consciência dessas razões sociológicas ou normativas: o sujeito age voluntariamente, conhecendo a dimensão jurídica da atuação. A vontade do negócio equivale ao desejo de desencadear os efeitos ou o conteúdo do negócio em causa[131].

Num processo de formação do contrato, o CC constrói um cenário de diálogo, entre as duas partes, que comporta duas eventualidades necessárias: uma proposta e uma aceitação[132].

2. Como fase necessária à formação de um contrato temos a proposta. Em termos formais, esta pode ser definida como *"a declaração feita por uma das partes e que, uma vez aceite pela outra ou outras partes, dá lugar ao aparecimento de um contrato"*[133]. A

[129] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Negócio jurídico*, 5ª ed., Almedina, 2023, p. 123.
[130] *Idem*, p. 125.
[131] *Idem*, p. 126.
[132] *Idem*, p. 318.
[133] *Ibidem*.

proposta contratual deverá reunir três requisitos essenciais: deve ser completa, deve revelar uma intenção inequívoca de contratar e deve revestir a forma requerida para o negócio em jogo[134].

O critério final para decidir da completude de uma proposta é a própria aceitação. Perante o artigo 232.º do CC, a proposta fica fechada quando a contraparte não suscite a necessidade de acordo sobre qualquer outro ponto[135].

3. A aceitação é uma declaração recipienda, formulada pelo destinatário da proposta negocial, cujo conteúdo exprima uma total concordância com o teor da declaração do proponente. Da aceitação resulta o contrato: não pode haver verdadeira aceitação quando a componente declaração surja dúbia ou condicionada. O contrato mais não é que um encontro das declarações confluentes das partes[136].

Assim, o contrato tem-se por celebrado quando a aceitação se torne eficaz, isto é, logo que chega ao poder do destinatário ou dele seja conhecida (artigo 224.º, n.º 1, com as especificações dos números 2 e 3 desse preceito do CC)[137].

4. À primeira vista, esta fase inicial do contrato não é muito diferente nos *smart contracts* e nos contratos tradicionais. Num contrato tradicional, ambas as partes têm de concordar no que diz respeito a um conjunto de cláusulas e a aceitação da proposta conduz à formação do contrato.

Apesar da semelhança de estrutura, existem diferenças que surgem com a natureza dos intervenientes. As partes num *smart contract* são representadas por uma morada, ou seja, são representadas por uma série de números[138]. Num contrato tradicional, a identidade dos intervenientes é, em regra, conhecida. Esta diferença não se revela substancial, tendo em conta que os contratos tradicionais não obrigam ao conhecimento entre as duas partes do negócio.

Paralelamente, um contrato tradicional pode requerer um tipo específico de representante como contraparte ou simplesmente alguém com capacidade legal, tema de que iremos

---

[134] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Negócio jurídico*, 5ª ed., Almedina, 2023, pp. 318 e 319.
[135] *Idem*, p. 321.
[136] *Idem*, p. 331.
[137] *Idem*, p. 333.
[138] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 21.

falar no próximo capítulo. Por exemplo, na rede *Ethereum*, qualquer um pode abrir uma conta sem necessitar de ter capacidade[139]. Assim, o individuo contraente terá de possuir capacidade jurídica para celebrar vários tipos de negócios no nosso sistema jurídico, mas aquele que celebra o seu contrato na rede pode não ter de preencher este requisito tendo em conta o desinteresse generalizado relativamente ao elemento da capacidade nas *blockchains*.

Apesar da identificação das partes através de moradas, o sistema acaba por não ser de absoluto anonimato, mas sim de pseudoanonimato. As partes identificam-se com base em técnicas criptográficas e o seu conhecimento uma da outra não é relevante em virtude da confiança na execução autonomizada[140]. À partida, as partes não podem ser obrigadas a revelar a sua identidade pois a confiança de que o contrato é celebrado no seu melhor interesse encontra-se no sistema da *blockchain*, como já tínhamos concluído.

Num *smart contract*, a aceitação chega no momento da realização de uma tarefa por parte da contraparte, mas ambas as partes têm também de concordar num clausulado inicial[141]. Existem, assim, duas hipóteses em matéria de aceitação. Por um lado, o código pode ser colocado numa rede como oferta, e com a realização de uma ação no sentido de aceitação, como ceder controlo a uma quantia pelo código, o contrato fica formado[142]. Por outro, duas ou mais partes podem desejar a formação de um contrato, acordando um clausulado, com recurso às linguagens de programação e posteriormente publicar o contrato na *blockchain*.

5. Em ambas as hipóteses, existe um acordo criado por ambas as partes ou aceite por uma delas que dá origem a um contrato. O facto de a confiança estar no sistema, no que diz respeito aos *smart contracts* que se encontram na *blockchain,* e nas partes no que

---

[139] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 21.
[140] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 83.
[141] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 322; MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019, p. 762.
[142] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, pp. 322 e 323.

diz respeito aos contratos tradicionais não invalida o facto de estruturalmente esta fase do processo contratual ser idêntica em ambas as realidades. Existe apenas um centro de confiança diferente.

10.1.2. Interpretação dos elementos de formação do contrato e o problema do erro

1. Em matéria de interpretação de negócios jurídicos, o CC dedica a este tópico três artigos: o artigo 236.º, o qual diz respeito ao sentido normal da declaração, o artigo 237.º, relativo a casos duvidosos e o artigo 238.º, relativo aos negócios formais.

O primeiro artigo indicado determina que *"a declaração vale com o sentido que um declaratário normal, colocado na posição do declaratário real, possa deduzir do comportamento do declarante, salvo se este não puder razoavelmente contar com ele"*. A ideia é que exista apoio no texto desenvolvido pelas partes, mas sejam tidas em conta as particularidades concretas do caso. O fim do negócio, o contexto em que o mesmo surge e o apelo à diligência do declaratário, ao nível do bom pai de família (artigo 487.º, n.º 1), são aspetos fulcrais nesta tarefa[143]. A segunda parte deste número, relativa à imputabilidade ao declarante, é uma forma de afastar certa interpretação se esta nada tiver a ver com a vontade do declarante[144]. O n.º 2 faz referência à vontade real, ao dizer que: *"Sempre que o declaratário conheça a vontade real do declarante, é de acordo com ela que vale a declaração emitida"*. Este preceito surge como forma de afastar a cegueira relativamente a uma mera declaração se for conhecida a vontade real do declarante. Independentemente disso, terá de existir uma declaração pois uma vontade real interior não pode fundamentar qualquer negócio[145].

O segundo artigo foi criado para auxiliar em casos de dúvida no que diz respeito ao sentido da declaração e varia consoante estejamos perante um negócio gratuito ou oneroso.

[143] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Negócio jurídico*, 5ª ed., Almedina, 2023, pp. 718-729.
[144] *Idem*, pp. 730-733.
[145] *Idem*, pp. 734 e 735.

No primeiro caso, prevalece o sentido que seja menos gravoso para o disponente e no segundo caso, prevalece o que conduza a um maior equilíbrio das prestações[146].

O terceiro artigo indicado estabelece uma regra especial de interpretação relativa aos negócios formais e determina que nestes negócios a declaração não pode valer num sentido que não apresente o mínimo de correspondência no texto, ainda que imperfeitamente expresso. Mas o n.º 2 dá-nos uma exceção: esse sentido pode valer se corresponder à vontade real das partes e se as razões determinantes da forma do negócio não se opuserem a essa validade[147].

2. No que diz respeito especificamente à interpretação do *smart contract,* será necessário determinar se o código pretendia definir obrigações ou apenas implementá-las. No primeiro caso, existe apenas um contrato em linguagem programática. No segundo caso, existe na base um contrato em linguagem tradicional que será executado ou completado por um *smart contract*. Tal irá afetar em muito o resultado da aplicação dos artigos de interpretação que analisámos acima.

Quando não exista um contrato em linguagem natural, apenas o código poderá determinar o sentido que as declarações teriam tendo em conta o parâmetro do programador razoável, atendendo à ausência de intervenção das partes no processo específico de redação do código. ANA PERESTRELO DE OLIVEIRA considera que os critérios do artigo 236.º do CC, mesmo que objetivados em função da tendência atual, não conduzem a um resultado efetivo. De qualquer forma, mesmo não existindo um contrato em linguagem natural é necessário interpretar o *smart contract* através da sua tradução para linguagem natural[148].

Esta autora apresenta dois métodos possíveis para fazer esta interpretação: ou atendendo à forma como um computador funcional entenderia o código, tendo em consideração os efeitos produzidos ou apelando ao sentido do código para o codificador razoável. Este apurará o código tendo em conta os efeitos de determinadas palavras no seu conjunto. O conceito de codificador razoável é um conceito novo, não se limitando este ao texto, mas

[146] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Negócio jurídico*, 5ª ed., Almedina, 2023, p. 742-749.
[147] *Ibidem*.
[148] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 58.

também ao contexto em que o mesmo foi redigido[149]. Também em sede de interpretação de contratos tradicionais não nos podemos cingir apenas à letra do texto, mas considerar também outros elementos circundantes.

Quando o *smart contract* execute o contrato tradicional, o problema de interpretação é distinto. Neste caso, a interpretação deve apelar ao conjunto para que se possa determinar se a linguagem natural se sobrepõe ao código ou se se complementam. Se a linguagem natural se sobrepõe ao código, o código só tem um objetivo de execução. Aqui o sentido do contrato é interpretado em termos gerais. O que conta é a vontade expressa no contrato em linguagem natural, a apurar nos termos do artigo 236.º do CC[150].

Se o sentido de o código não coincidir com a vontade expressa no contrato em linguagem natural, o programador de duas uma: ou interpretou erradamente este contrato ou existe um erro na programação. Em qualquer caso, não revela o conceito do programador razoável. O que terá de se determinar nesta sede é se o que se programou corresponde ao sentido do contrato tradicional, tendo em conta as regras gerais de interpretação, mas sempre tendo em conta o *smart contract*. Se o código não corresponde de facto ao contrato tradicional, prevalece este último. Esta incongruência entre os clausulados deve justificar a intervenção do sistema jurídico[151].

Se o *smart contract* for um complemento ao contrato tradicional, deverá analisar-se o conjunto. Nesta tarefa de interpretação, o juiz terá de traduzir este contrato para linguagem natural e analisá-lo com analisaria qualquer outro. Apesar disso, considera-se que, em termos ideais, o *smart contract* deve conter regras para a sua interpretação de forma a facilitar este processo[152]. A função aqui já não é apenas de reproduzir o contrato tradicional noutra linguagem, mas sim adicionar algo ao clausulado em linguagem natural já existente.

3. Sabemos que em qualquer negócio poderá haver engano de qualquer uma das partes que o celebre. O erro implica, em termos gerais, uma avaliação falsa da realidade,

[149] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 59 e 60.
[150] *Idem*, p. 60.
[151] *Idem*, pp. 60 e 61.
[152] *Idem*, pp. 61 e 62.

seja por carência de elementos, seja por má apreciação destes e, num outro caso, por atuação própria ou por intervenção, maldosa ou inocente, das partes ou de terceiros. Para além destas situações, podemos ter a situação em que ocorre a formação adequada da vontade, mas surge um obstáculo à sua exteriorização ou comunicação[153].

No tópico do erro podemos dizer que a utilização de código pode minimizar conflitos no que diz respeito aos termos acordados. Apesar de existir também ambiguidade na linguagem de programação, essa ambiguidade é muito menor do que no contexto contratual tradicional pelo facto da linguagem humana ter uma maior variedade de formas de expressar a mesma realidade. Uma linguagem de computador ambígua é um conceito que choca com a previsibilidade destas máquinas[154].

Como mencionámos no parágrafo anterior, não há uma completa irradicação da possibilidade do erro na linguagem programática. HUGO RAMOS ALVES chama-nos a atenção para o facto de o legislador português admitir três situações distintas neste contexto, com base nas construções de erro já existentes, mas adaptadas a esta realidade: erro na programação, defeito de funcionamento da máquina e erro na transmissão[155].

- Nos casos de erro na programação, estaremos perante uma situação em que é aplicável o erro na formação da vontade. Nestas situações, a vontade em que assentou a base da programação está viciada de erro ou, ainda, situações em que, apesar de se pretender introduzir uma determinada informação, foi introduzida informação diversa. Assim, poderemos, em teoria, proceder à aplicação do regime de erro-vício. Todavia, a aplicação pode ser problemática, nomeadamente em casos de erro sobre a pessoa, pois o requisito de essencialidade do conhecimento ou dever de conhecimento apenas pode ser invocado quando o declaratário seja uma pessoa

[153] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Negócio jurídico*, 5ª ed., Almedina, 2023, p. 835.
[154] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, pp. 324 e 325.
[155] HUGO RAMOS ALVES, "Smart Contracts: Entre a tradição e a inovação" em *Fintech II – Novos Estudos sobre a Tecnologia Financeira*, António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (coord.), Almedina, 2019, pp. 207 e 208; LAWRENCE AKKA / SAM GOODMAN / MATTHEW LAVY *et. al., Legal Statement on Cryptoassets and Smart Contracts*, UK Jurisdiction Taskforce, disponível em https://technation.io/about-us/lawtech-panel, 2019, p. 35.

física. Caso o declaratário seja um autómato, este não se poderá aperceber do processo formativo da vontade, atento o facto de apenas estar programado para executar o código;

Apesar da contratação envolver pessoas físicas por detrás de computadores, a execução é feita por um sistema. O executor irá apenas executar o contrato como este foi colocado na plataforma, não tem capacidade para analisar o processo da vontade. Nos casos em que a vontade em que assentou a base da programação está viciada de erro podemos reconduzir esse erro aos contraentes, mas nas situações em que, apesar de se pretender introduzir uma determinada informação, foi introduzida informação diversa está em causa o criador do código que será um *coder*.

- Na eventualidade de ocorrer um defeito de funcionamento da máquina, tal poderá implicar que a declaração não seja emitida em conformidade com a programação por erro do instrumento utilizado para redigir o código. Trata-se de algo semelhante ao erro na declaração. Neste caso, estaremos novamente perante dificuldades de ordem prática: exigindo-se, por um lado, no artigo 247.º do CC, que *"o declaratário conhecesse ou não devesse ignorar a essencialidade, para o declarante, do elemento sobre que incidiu o erro"* e, por outro, que sendo em abstrato possível lançar mão do regime vertido no artigo 249.º, dificilmente tal será exequível. O simples erro de cálculo ou escrita dificilmente será apreendido pelo autómato e o regime dos artigos 247.º e seguintes pressupõe pessoas físicas, pelo que, numa situação de contratação multilateral automatizada, dificilmente o mesmo será relevante, pois o autómato só responde pela execução do programa tal como inserido pelo seu criador;
- Estaremos perante um erro na declaração quando o código é emitido, mas chegou deformado ao destino. Também aqui a concreta verificação dos requisitos será de difícil aplicação, tendo em conta que o autómato não está programado para sindicar as declarações recebidas[156].

[156] HUGO RAMOS ALVES, "Smart Contracts: Entre a tradição e a inovação" em *Fintech II – Novos Estudos sobre a Tecnologia Financeira*, António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (coord.), Almedina, 2019, pp. 208 e 209.

4. O autor considera que estes sistemas são de difícil aplicação no meio da *blockchain*, tendo em conta a multilateralidade de algumas relações contratuais e a existência de um autómato sem vontade que apenas segue aquilo para o qual foi programado.

Este regime do CC está pensado para lidar com duas vontades em confronto, duas vontades que pertencem a duas pessoas físicas. Nesta lógica, o autor considera que é interessante a tese avançada a propósito da LCE por Paula Costa e Silva. De acordo com a autora, uma vez que estamos perante situações baseadas no benefício e no risco, em caso de defeito, compete ao programador assumir os riscos do funcionamento do programa[157].

Esta solução é considerada excessiva pelo autor tendo em conta a natureza excecional da imputação pelo risco, nos termos do artigo 483.º, nº 2 do CC. Em qualquer caso considera possível, contanto que exista um contrato e os requisitos do erro não se verifiquem, recorrer à responsabilidade contratual; não sendo possível descortinar o erro vício ou mesmo um erro obstáculo, teremos de atender a aspetos consequenciais, como, por exemplo, à eventual responsabilização da parte que transmitiu e que utilizou a máquina em proveito próprio[158].

5. O facto de estarmos perante contratos que são pensados por duas partes humanas, mas posteriormente executados por um sistema levanta problemas ao nível da análise da sindicalização do erro. Mas, como vimos, tanto em matéria de interpretação no geral, como em matéria de erro no específico, as partes estão afastadas do processo de redação e claro de posterior execução. Estas apenas enviam os elementos contratuais para o programador para que ele possa traduzir o contrato para código. O programador é que poderá ser responsabilizado nesta sede.

[157] HUGO RAMOS ALVES, "Smart Contracts: Entre a tradição e a inovação" em *Fintech II – Novos Estudos sobre a Tecnologia Financeira*, António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (coord.), Almedina, 2019, p. 209.
[158] *Idem*, p. 210.

10.2. Requisitos formais

1. Como sabemos, existe um princípio de liberdade de forma no nosso direito dos contratos. Desde que não existam fatores que impeçam a formação do contrato como vícios, a forma não é relevante maior parte das vezes. Podemos considerar que a utilização do modelo de *smart contract* representa uma escolha implícita das partes em usar uma forma especial para formar um contrato[159].

Um *smart contract* permite introduzir todo o tipo de regras na eventualidade de diversos comportamentos de cada uma das partes. Tecnicamente, não existe possibilidade de arrependimento de certas promessas realizadas tendo em conta que a máquina executará as ações para a qual foi programada[160].

2. De forma a explicar como funcionam os *smart contracts* na prática, NICK SBAZO utiliza a analogia da máquina *vending*. A máquina aceita as moedas introduzidas e entrega o produto de acordo com o preço no mostrador. A partir do momento em que as moedas são inseridas, não é necessária mais intervenção humana para executar o contrato. Mesmo que, por exemplo, a pessoa fosse forçada a introduzir as moedas na máquina, iria adquirir o produto. A vontade pode encontrar-se em perigo num momento posterior à formação do contrato[161].

10.3. Capacidade

1. As partes, numa relação contractual, devem ser dotadas de capacidade jurídica para que esta seja eficaz. Contudo, maior parte das *blockchains* não verificam a capaci-

[159] GABRIEL OLIVIER BENJAMIN JACCARD, *Smart Contracts and the Role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017, p. 23.
[160] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 233.
[161] MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019, p. 757.

dade dos seus intervenientes. Como os *smart contracts* não têm forma de testar a capacidade dos indivíduos, estes poderão ser colocados na *blockchain*, por exemplo, por menores.

Recorrendo novamente à analogia da máquina *vending*, Nick Sbazo diz-nos que, em teoria, qualquer pessoa com moedas pode comprar o produto, independentemente de ter ou não capacidade legal para o fazer. Desde que ambas as partes aceitem o *smart contract*, a sua execução está fora do seu controlo[162]. Aceitar o *smart contract* significa aceitar o risco de que a contraparte não tenha capacidade para o negócio.

A rede *blockchain*, ao permitir a entrada de quaisquer indivíduos, independentemente da sua capacidade jurídica, conduz a que estes indivíduos tenham essa realidade em conta quando vão contratar. Pelo que não nos parece que possa haver uma invalidação do contrato com base na incapacidade de qualquer uma das partes. O risco terá sido assumido no sentido de aceitação da possibilidade de celebração de um negócio com um incapaz.

10.4. Modificação

1. Uma obrigação é modificada sempre que sofra uma alteração que não acarrete uma quebra de identidade. Uma alteração em qualquer situação obrigacional complexa requer uma modificação objetiva seja na posição do credor, seja na do devedor, seja no vínculo. Por isso, modificações que se limitem a proceder à substituição de sujeitos, sem provocar inovações nas situações jurídicas em si não devem ser consideradas modificações para estes efeitos como nos diz ANTÓNIO MENEZES CORDEIRO[163].

A manutenção da identidade de uma obrigação depende, fundamentalmente, da conservação da prestação. Podemos entender que uma obrigação é a mesma quando a conduta devida nela em causa seja, também, a mesma. O problema desloca-se para a prestação:

[162] MANTEJA DUROVIC / ANDRÉ JANSSEN, *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019, p. 757.
[163] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das obrigações, cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, Almedina, 2016, p. 417.

ocorrida uma modificação objetiva em determinada obrigação, só se poderá falar em modificação *proprio sensu* quando a prestação devida se mantenha[164].

Não quer dizer que a prestação não possa sofrer alterações. Essas alterações não devem ser tais que conduzam a que, da mesma prestação, já não caiba falar. O critério para determinar se se está perante a mesma prestação é extrajurídico. Desde logo, depende da linguagem: haverá uma mera modificação quando a prestação alterada possa ser vinculada pelas mesmas locuções vocabulares. A manutenção linguística é uma continuidade de regime jurídico. Salvo qualquer disposição normativa que comine solução diferente, o regime acomodar-se-á, depois, à solução extrajuridicamente indicada[165].

Nas alterações das obrigações podem ser visadas tanto as posições fundamentais dos sujeitos da obrigação, como aspetos meramente acessórios, complementares ou instrumentais. Pode ser alterado, por exemplo, o conteúdo da prestação principal, o seu montante, o tempo e local do cumprimento, as prestações secundárias ou os deveres acessórios[166].

De acordo com a área da obrigação alterada, podemos distinguir modificações de objeto e modificações do conteúdo. Modificações de objeto são aquelas que respeitam à prestação; modificações do conteúdo, pelo contrário, são as que deixam incólume a prestação e reportam tão-só a outros aspetos do normativo obrigacional[167].

Qualquer modificação é um efeito jurídico. Consequentemente, pressupõe a aplicação de normas desencadeadas pela verificação de factos jurídicos. Estes factos são factos modificadores. Podemos distinguir estas modificações em modificações voluntárias e legais, consoante sejam provocadas por ato jurídico ou por facto *strictu sensu*. É regra quase absoluta do nosso sistema jurídico as obrigações terem de ser sempre acompanhadas pelas fontes respetivas, isto é, pelos factos constitutivos, de acordo com o princípio de causalidade. Tal explica-se pela natureza do vínculo obrigacional, pois este só é reconhecido

[164] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das obrigações, cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, Almedina, 2016, p. 417.
[165] *Idem*, pp. 417 e 418.
[166] *Idem*, p. 418.
[167] *Idem*, p. 419.

através da sua fonte. Da mesma forma, operada uma modificação em determinada obrigação, esta passa a ser comandada pela fonte e pelo facto modificativo, o que quer dizer que o próprio facto modificativo surge como modificado[168].

A grande maioria das modificações creditícias, tendo em conta a relevância do princípio da autonomia privada no nosso direito das obrigações, tem natureza voluntária. Em princípio, as partes podem, por simples acordo, no respeito por diversas limitações nomeadamente as de ordem formal modificar as obrigações contratuais que tenham criado. Na prática, processam-se através de alterações introduzidas no contrato inicial, via um novo contrato[169].

2. A possibilidade de modificação existe no direito contratual tradicional, como vimos no parágrafo anterior, nomeadamente por força de uma alteração de circunstâncias, mas cabe aqui determinar se essa possibilidade se estende aos *smart contracts*[170].

Um bom *smart contract* coloca a probabilidade de subversão oportunista perto do zero pois tais comportamentos são impossíveis ou demasiado dispendiosos. Os *smart contracts* incluem protocolos segundo os quais as partes agem com base em promessas, sendo estes executados automaticamente, sem a necessidade de intervenção de intermediários ou do poder judicial[171].

Da existência destes protocolos resulta uma ideia de segurança e a única forma de quebrar estas promessas contratuais passa por atacar a tecnologia que lhes serve de base. O problema que surge com esta segurança é a impossibilidade de resolução de qualquer problema que surja depois do início da execução, tanto uma circunstância posterior à execução como uma circunstância existente já à data de execução, mas que nunca foi detetada. No contexto da execução de um contrato, as circunstâncias podem mudar, nomeadamente pode ocorrer uma mudança de preços que pode degradar o valor do contrato para as partes contratantes. Pode também existir um erro ortográfico ou de outro tipo no contrato, como

---

[168] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das obrigações, cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, Almedina, 2016, p. 419.
[169] *Idem*, pp. 419 e 420.
[170] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Technology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 326.
[171] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, pp. 151 e 152.

já analisámos, encontrando-se as partes com o desejo de proceder à alteração do clausulado[172].

No direito contratual existem diversas possibilidades de modificação ou término de um contrato. Por isso, parece-nos necessário definir novos padrões para que estas ferramentas possam ser aplicadas aos *smart contracts* de forma eficiente[173].

A resolução e mesmo a modificação no plano contratual tradicional são efetivados através da declaração de uma das partes à outra, o que não é possível no contexto da *blockchain* por força da imutabilidade que caracteriza os *smart contracts* a partir do início da sua execução. Este aspeto faz com que se afaste a possibilidade de aplicação do instituto de alteração de circunstâncias ao *smart contract* que habita na *blockchain*[174].

Quando existam circunstâncias que desequilibrem o contrato teremos de analisar se a solução será a mesma com base na ligação do contrato ao exterior ou não. Num contrato totalmente automatizado, a indiferença das circunstâncias exteriores é absoluta. Estando o contrato apenas ligado à *blockchain*, a modificabilidade entrará em choque com a confiança depositada no sistema. A irrelevância da alteração das circunstâncias nos *smart contracts* quando tal não tenha sido programado não vai contra o sistema jurídico. Para estes, o único limite será a boa-fé. A impossibilidade de alteração significa que os riscos da realidade fazem parte dos riscos dos contratos por força da ligação da *blockchain*[175].

A alteração das circunstâncias anda ligada com a relação de confiança entre as partes. As partes assumem o risco de desequilíbrio quando optam pelo recurso a um sistema contratual caracterizado pela sua rigidez e incapacidade de adaptação. O alheamento à realidade mutável é precisamente consequência da abstração que caracteriza a *blockchain*[176].

Na ausência de diferente programação, o risco da realidade recai sobre as partes cuja esfera jurídica seja afetada. A escolha pela imutabilidade é um exercício da autonomia

[172] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, p. 152.
[173] *Ibidem*.
[174] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 75.
[175] *Idem*, pp. 75 e 76.
[176] *Idem*, p. 77.

das mesmas pelo que só podem alegar que não contavam com esta distribuição de risco e nesse caso estaremos perante um problema de erro, a ser analisado noutra sede[177].

Existem, contudo, casos extremos que poderão exigir a modificação ou cessação de um contrato. A autora ANA PERESTRELO DE OLIVEIRA apresenta algumas soluções para descreditar esta ideia de absoluta irreversibilidade dos *smart contracts*. Uma das soluções será através da realização de uma transação inversa. Apesar de não ser possível alterar blocos já existentes será possível adicionar novos blocos que revertam transações anteriores. Em sentido técnico, acaba por não ocorrer uma modificação ou destruição dos dados, mas sim a adição de nova informação que reflita corretamente a situação real no contexto da *blockchain*. Isto conduz à existência de duas situações que se podem anular uma à outra[178].

No caso de uma transação inversa, tudo se passa como se a transação fosse realizada de novo, mas com um sinal oposto, pelo que está necessariamente dependente da cooperação da contraparte[179].

Outra possibilidade apresentada pela autora é a modificação através de um *hard fork*, situação que já analisámos acima nesta investigação. Este representa uma cisão entre duas redes, ordenada de forma a fazer prevalecer a rede com a informação correta nesse momento. O *fork*, tal como a transação inversa, também não apaga ou modifica dados prévios. Apesar disso, tem-se por preferível a solução das transações inversas para estas situações extremas de alteração ou cessação. Contudo, a solução mais célere e económica será a restituição em espécie ou de valores correspondente, sem prejuízo do artigo 432.º, n.º 2. do CC[180].

Nos casos em que as circunstâncias tenham sido alteradas de forma que o risco normal ligado à imutabilidade é ultrapassado, pode ser determinar um dever de renegociação especificamente em cenários em que a programação originária deixa de ter correspondência com a realidade. Este dever tem em vista a reposição do equilíbrio modificado[181].

---

[177] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 78.
[178] *Idem*, pp. 79 e 80.
[179] *Idem*, p. 82.
[180] *Idem*, pp. 83 e 84.
[181] *Idem*, pp. 85 e 86.

Em caso de incumprimento deste dever existe responsabilidade civil, sendo a solução indemnização a solução a adotar. A indemnização poderá ser em espécie, caso em que o tribunal ordena uma transação invertida, ou em dinheiro[182].

3. Por outro lado, ARI JUELES e BILL MARINO desenvolveram um estudo interessante sobre várias formas de alteração e decidiram testar a sua teoria na plataforma *Ethereum*.

Resumindo, os autores identificam três formas de modificação que facilmente podemos associar às categorias de modificação do nosso sistema. Serão estas a modificação legal onde as cláusulas de modificação atribuem o direito a uma das partes de corrigir o contrato; a modificação voluntária, sendo a modificação um contrato por si próprio e tendo por base um acordo mútuo; e, por fim, aquilo que podemos equiparar a uma medida coerciva de modificação com base na boa-fé, na qual um tribunal pode ordenar a modificação, mesmo contra objeções de uma ou mais partes quando ocorram erros mútuos a todas as partes, fraude ou termos criados com uma vantagem irrazoável para uma das partes[183].

Os requisitos comuns a todos estes mecanismos são a suspensão da performance dos termos iniciais, o início da performance dos termos modificados e a compensação parcial pela performance já ocorrida.

- A modificação por direito deve suspender a performance dos termos que se pretende modificar e simultaneamente iniciar a performance dos termos modificados. Os requisitos especiais desta forma de modificação são a vontade na modificação de um termo por parte do contraente com o direito a fazê-lo e se a modificação for condicionada à ocorrência de certos eventos, esses eventos devem ocorrer depois da modificação e apenas se as condições de modificação estiverem preenchidas.
- A modificação por acordo, como requisito especial, exige que esta apenas seja possível quando todas as partes concordem com a modificação.
- A reforma apresenta algum interesse para os *smart contracts*, tendo em conta a maior probabilidade de desvio acidental da vontade das partes num acordo escrito,

[182] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 87.
[183] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, pp. 155-158.

por força da introdução do código. Como requisito especial, exige que esta apenas possa ser permitida quando iniciada pelo tribunal adequado[184].

A *blockchain* da *Ethereum* armazena tanto dados de transação relativos à criptomoeda *Ether*, como *smart contracts*. Os nós na rede *Ethereum*, para além de adicionarem transações à rede, também iniciam a execução do código, mantêm e ajustam o estado dos contratos numa máquina virtual, a máquina virtual *Ethereum*[185].

Contratos em *Ethereum* podem conter *Ether*. Como objetos num tipo de programação orientada pelo objeto, podem conter variáveis e funções que podem ajustar essas mesmas variáveis ou realizar outras atividades como enviar *Ether* para outros contratos e contas dentro da rede *Ethereum*[186].

4. A modificação de contratos no *Ethereum* tem mais nuances do que a cessação. Existem três formas de modificar os contratos em *Ethereum*: modificação de termos variáveis, eliminação de termos relacionados com função e adição ou alteração de termos relacionados com função[187].

De forma a contextualizarmos certos aspetos que vamos mencionar de seguida, temos de fazer referência aos métodos de cessação dos contratos nomeadamente a resolução em termos clássicos, a rescisão por acordo e por decisão judicial. Os requisitos gerais e comuns a todos estes são a suspensão da performance e a compensação da performance parcial já ocorrida. A resolução em termos clássicos tem como requisitos especiais o desejo da parte com o direito para tal para ativar a medida e a satisfação de todas as condições de resolução. A rescisão por acordo tem como requisito especial o acordo de todas as partes para ser ativada. A rescisão por ação judicial tem como requisito especial a atuação do tribunal adequado para ser ativada[188].

Termos contratuais como preços podem ser considerados variáveis em código. Quando esse é o caso, modificar os termos é tão simples como atribuir um novo valor à variável, utilizando uma função. Se essa função existir, o método de modificação é suficiente para preencher o primeiro requisito deste instrumento: interromper a performance do termo

[184] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, pp. 155-158.
[185] *Idem*, p. 158.
[186] *Ibidem*.
[187] *Idem,* p. 162.
[188] *Idem*, pp. 153-155.

antigo e iniciar a performance do novo. Se a função for adequada a esta variável, este método satisfaz também o segundo requisito de resolução em termos clássicos: o essencial deve ser codificado no *smart contract* durante a sua formação. Os demais requisitos das diferentes formas de modificação podem ser preenchidos da mesma forma que são preenchidos na resolução em termos clássicos, na rescisão por acordo e por decisão judicial[189].

Mas nem todos os termos contratuais são variáveis. Neste caso, a modificação significa eliminar, adicionar ou trocar uma função relevante. Esta situação terá de ser resolvida de forma diferente pois, ao contrário das variáveis que podem ser alteradas livremente, as funções num código de contrato *Ethereum* são imutáveis a partir do momento em que o contrato é emitido na *blockchain*[190]*:*

- A função mais fácil de implementar será a eliminação. Para tal, podemos utilizar os modificadores para criar estados, fazendo com que as funções determinem exceções caso não se verifiquem esses mesmos estados. Utilizando este método, criaremos funções que possam ser desligadas caso as partes concordem com um sistema de eliminação. Tal irá bloquear a performance, o que preenche o primeiro requisito. Os demais requisitos podem ser preenchidos como são nos termos variáveis[191].
- As funções de adição e modificação são acionadas de forma semelhante. Existe apenas uma diferença: quando uma função é substituída, a sua versão inicial deverá também ser desligada. Na *Ethereum*, existem pelo menos duas formas de adicionar e trocar funções. A primeira reside na possibilidade de ligar novamente as funções com a utilização destes modificadores. Para puderem ser ligadas, as funções devem estar originalmente no contrato. Como o código é imutável a partir do momento da sua formação, tal significa que as funções que as partes pensam eventualmente ligar durante a modificação devem ser incluídas no contrato num modo desligado. Se tal for alcançado, os requisitos das três formas de modificação contratual estão preenchidos. Uma segunda maneira de adicionar ou modificar é

[189] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, p. 162.
[190] *Idem*, pp. 162 e 163.
[191] *Ibidem*.

criando contratos-satélite que representem certas funções. As moradas dos diversos contratos-satélite devem ser armazenadas nas variáveis de morada ou um conjunto destas num contrato central. Assim, quando seja necessário referenciar certos termos, o contrato central pode remeter para o contrato-satélite[192].

5. Este último modelo é apresentado como forma de resolver o problema de impedimento de modificação ou cessação de *smart contracts* por força da imutabilidade que caracteriza o sistema que tem estes por base. Na própria exposição relativamente às soluções para a rede *Ethereum*, vemos a necessidade de estes elementos terem de constar do clausulado inicial de forma a serem ativados ou desligados, tendo em conta que após o início da execução nada mais pode ser adicionado. Para além desse aspeto, a suspensão da performance, elemento comum à implementação de todas estas soluções, é um conceito completamente contrário à natureza imutável e imparável da *blockchain*. Por isso, nesta sede iremos adotar a posição da autora ANA PERESTRELO DE OLIVEIRA e admitir a modificação e cessação apenas em casos excecionais.

10.5. Incumprimento

1. O cumprimento é a realização da prestação devida duma obrigação, nos termos do artigo 397.º do CC. Isto mesmo esclarece o artigo 762.º, n.º 1 do CC que nos diz que *"o devedor cumpre a obrigação quando realiza a prestação a que está vinculado"*. Só há cumprimento, porém, se a pessoa que cumpre for o devedor ou se a pessoa que cumpre o fizer em lugar do devedor, ou seja, por ordem ou indicação do devedor, declarando que cumpre pelo devedor ou agindo à custa dele– por exemplo, entregando um bem que pertence ao devedor ou lhe pertencia até àquele momento. O indivíduo em causa deverá ter legitimidade para efetuar ou receber a prestação, caso contrário não haverá extinção da obrigação[193].

Ao cumprimento reconhece-se tradicionalmente um efeito extintivo. A obrigação extingue-se, o devedor fica exonerado quando cumpre exatamente conforme devia. Assim, nas

[192] ARI JUELES / BILL MARINO, *Setting standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016, p. 163.
[193] LUÍS MENEZES LEITÃO, *Direito das Obrigações II – Transmissão e Extinção das Obrigações; Não Cumprimento e Garantias de Crédito*, 11ª ed., Almedina, 2017, p. 148.

obrigações de meios, é muito comum que o devedor tenha de continuar a tentar alcançar o resultado pretendido enquanto não deixar de ser possível alcançá-lo ou for impossível fazê-lo, embora todos os atos sejam atos de cumprimento. Nas obrigações negativas, também é comum que a abstenção tenha de ser mantida ou repetida. Mesmo nas obrigações irrepetíveis, o cumprimento não extingue a obrigação nos casos de sub-rogação, nos termos dos artigos 589 e seguintes do CC.

2. Por oposição, haverá não cumprimento sempre que não seja realizada uma prestação devida enquanto devida[194]. Em sentido amplo, o incumprimento contratual abrange o incumprimento definitivo, a mora do devedor que consiste no atraso da realização da prestação, sendo esta ainda possível, e o cumprimento defeituoso que ocorre quando há violação do direito de crédito que não integra a mora ou o incumprimento definitivo, nomeadamente quando o devedor realiza a prestação a que está adstrito com irregularidades. LUÍS MENEZES LEITÃO oferece-nos uma boa definição de não cumprimento ao afirmar que este representa *"a não realização da prestação devida por causa imputável ao devedor, sem que se verifique a extinção da obrigação"*[195].

No caso de incumprimento definitivo, a consequência principal será a constituição do devedor em responsabilidade obrigacional pelos danos causados pelo credor (artigo 798.º do CC). Terá de haver um facto ilícito, a não execução terá de ser imputável ao devedor, é necessário que o credor sofra danos e que haja um nexo de causalidade entre esses danos e o não cumprimento por parte do devedor. A impossibilidade da prestação é equiparada por lei ao incumprimento contratual definitivo. Se a prestação for impossível por culpa sua, pode responder como se faltasse culposamente ao cumprimento da obrigação. Admite-se que as partes estipulem um regime de responsabilidade pelo incumprimento contratual. Elas podem fixar em acordo prévio quer os pressupostos da responsabilidade quer o montante da indemnização.

Por fim, resultando a obrigação de um contrato bilateral, existe a hipótese do credor exercer a sua faculdade de resolução, podendo exigir também a restituição em inteiro da contraprestação, se já a tiver efetuado.

---

[194] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, Almedina, 2016.p. 210.

[195] LUÍS MENEZES LEITÃO, *Direito das Obrigações II – Transmissão e Extinção das Obrigações; Não Cumprimento e Garantias de Crédito*, 11ª ed., Almedina, 2017, p. 225.

Havendo incumprimento num contexto de prestações recíprocas, num contrato sinalagmático como a compra e venda, podemos ter uma de duas situações. Poderá haver recusa do cumprimento que se encontra prevista no artigo 428.º que, no seu n.º 1, nos diz que *"não havendo prazos diferentes de cumprimento das prestações, cada contraente tem o direito de recusar a sua prestação enquanto o outro não efetuar a sua ou não oferecer o seu cumprimento simultânea";* outra consequência possível do não cumprimento neste contexto é a resolução que resulta do artigo 801.º, n.º 2 do CC.

3. Idealmente, um *smart contract* incluiria no seu código todas as hipóteses de incumprimento, programando determinadas consequências automáticas na sua ocorrência. Contudo, sabemos já, por experiência com os contratos tradicionais, que a discriminação de todas as hipóteses de incumprimento é impossível tendo em conta o elevado volume de possibilidades[196].

Cabe então saber se o sistema da *blockchain* poderá substituir o sistema jurídico e quais os meios de que o ordenamento jurídico dispõe para controlar a incorporação dessas estratégias de resolução de litígios dos *smart contracts*. Como sabemos, a automatização dos *smart contracts* e a promessa de performance garantida não diminuem o recurso aos tribunais do Estado. Uma forma possível de contornar o problema dos meios de litígios a aplicar será através da integração de meios alternativos de resolução de litígios no próprio contrato. De forma a manter a resolução de litígios dentro do meio digital, a autora ANA PERESTRELO DE OLIVEIRA sugere a necessidade de novos modelos de arbitragem, denominados de *smart arbitration*. Uma arbitragem que se executa automaticamente[197].

A autora constrói possíveis meios de resolução de litígios dentro da *blockchain* nomeadamente através de *crowdsourcing*. Contudo já existe uma forma de resolução de litígios dentro da *blockchain Bitcoin*: o sistema de endereço de assinaturas múltiplas. Este consiste numa espécie de fechadura que só se abre se forem usadas as duas chaves relevantes na transação. Havendo um desentendimento, nenhuma das partes usará a sua chave, ficando os efeitos da transação suspensos. Estas terão de recorrer a um terceiro que decidirá

[196] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, p. 63.
[197] *Idem*, pp. 67 e 68.

a questão através da utilização de uma chave que só poderá ser utilizada em conjunto com as duas outras[198].

A autora explora também as situações de impossibilidade, que no nosso direito serão equiparáveis ao incumprimento se essa impossibilidade for total, distinguindo entre os contratos totalmente automatizados e os contratos com elementos *off-chain*. Nestes primeiros, as situações de impossibilidade são raras e podem-se traduzir nos casos em que o próprio código não pode ser executado de todo ou como as partes desejaram que fosse. Não sendo a prestação executada por razões de força maior, não há incumprimento imputável. De forma a determinar a solução indicada terá de se analisar se estamos perante um incumprimento definitivo ou temporário ou se estamos perante uma situação de impossibilidade, pois a impossibilidade de execução não exclui a possibilidade de execução fora da *blockchain*[199].

Caso o contrato tenha elementos *off-chain*, a impossibilidade implica uma falha da informação transmitida pelo oráculo que posteriormente não desencadeia os efeitos de execução da prestação dependente de condição. Neste caso, não há incumprimento tendo em conta a verificação de uma circunstância de força maior[200].

4. Por não ser ainda possível identificar a existência de um sistema próprio de resolução de litígios próprio da *blockchain* fará sentido recorrer aos tribunais do Estado, visto que tal não é impossível. Havendo incumprimento no meio contractual, a parte prejudicada poderá dirigir-se ao tribunal ou a um meio de defesa similar e exigir uma indemnização por danos patrimoniais ou a repetição do indevido em casos de enriquecimento causa[201].

A existência de um sistema judicial público que puna também aqueles que incumpram os seus *smart contracts* parece em tudo contrário à identidade de um sistema descentralizado dentro do qual estes contratos surgem[202]. Por isso, estão a ser realizados esforços para

[198] ANA PERESTRELO DE OLIVEIRA, *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial – Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023, pp. 71 e 72.
[199] *Idem*, pp. 72 e 73.
[200] *Idem*, p. 73.
[201] MAX RASKIN, *The Law and Legality of Smart Contracts*, Georgetown Law Techonology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017, p. 321.
[202] *Idem*, p. 329.

construir um sistema para lidar com problemas nomeadamente de incumprimento dentro da própria rede.

5. Em suma, tendo em conta a assimilação do *smart contract* no conceito de contrato e consequente integração no sistema jurídico que pretendemos aqui defender, fará todo o sentido que, enquanto não exista um sistema de resolução de litígios próprio da *blockchain*, seja possível que a parte afetada possa recorrer às entidades judiciais competentes a nível estadual.

11. NEGÓCIOS DE TRANSMISSÃO DE CRIPTOATIVOS

11.1 Contrato de compra e venda: generalidades

1. A noção de compra e venda consta do artigo 874.º do CC. O teor do artigo é o seguinte:

"Compra e venda é o contrato pelo qual se transmite a propriedade de uma coisa ou direito mediante um preço".

Com base nesta afirmação é possível identificar dois elementos essenciais desse contrato: a transferência da propriedade de uma coisa ou direito e pagamento de um preço. Estes elementos fazem também parte, por força do artigo 879.º do CC, dos efeitos essenciais do contrato de compra e venda. São estes, por um lado, um efeito real de transferência da titularidade de um direito e, por outro, dois efeitos obrigacionais, a obrigação, por parte do comprador, de pagar o preço e a obrigação pendente sobre o vendedor de entregar a coisa vendida[203].

Dentro destes limites vale, como regra, o princípio da liberdade contratual consagrado no artigo 405.º do CC. As partes podem estabelecer o conteúdo que entenderem conquanto no respeito pelos elementos essenciais do contrato. Podem existir, todavia, alguns limites, a maior parte das vezes relacionados com o bem objeto da compra e venda, com necessidades especiais de proteção do consumidor ou proteção da concorrência entre agentes económicos[204].

A compra e venda é um contrato típico e nominado, ou seja, as suas cláusulas nucleares constam da lei e este tem uma designação própria fixada na lei. Consiste ainda num contrato consensual, em oposição ao contrato real *quoad constitutionem*. Quer isto dizer que não se encontra associada à constituição ou celebração do contrato a entrega da coisa. O

[203] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, pp. 68 e 69.
[204] *Idem*, pp. 69 e 70.

contrato surge imediatamente com o encontro da vontade das partes, antes da entrega da coisa[205].

O contrato de compra e venda é um contrato causal. O princípio da causalidade diz-nos depender a constituição ou modificação de direitos reais da existência, da validade e da procedência da causa jurídica na ordenação das situações jurídicas[206].

O contrato de compra e venda está sujeito às regras gerais dos artigos 217.º e seguintes relativamente à forma. Como já vimos, vale o princípio de liberdade de forma, mas, em alguns casos, a lei exige a observância de forma específica como é o caso da compra e venda de coisas imóveis que não nos interessa explorar nesta dissertação.

2. Na compra e venda, a transmissão da propriedade é gerada ou provocada pelo próprio contrato e depende exclusivamente dele. No CC, a eficácia da compra e venda decorre dos artigos 408.º, 874.º e 879.º, alínea a). Quanto à transferência da posse, se não se assistir a uma tradição da coisa, real ou simbólica, a posse só poderá ser transferida com o constituto possessório (artigo 1264.º do CC)[207].

De acordo com o artigo 408.º do CC, *"salvas exceções previstas na lei"* a constituição ou transferência de direitos reais sobre coisa determinada dá-se por mero efeito do contrato. Ou seja, como regra a compra e venda é dotada de eficácia real e como exceção é uma venda obrigacional, dependendo de ato translativo ou constitutivo posterior ao contrato[208]. Em conclusão, no nosso direito civil, a compra e venda tem sempre carácter real. Um contrato do qual não decorra a transmissão da titularidade de uma coisa ou direito não poderá nunca qualificar-se como compra e venda civil; mesmo quando reunidos e verificados os demais requisitos e efeitos deste contrato[209].

3. Como vimos, temos dois efeitos obrigacionais. Começando pela obrigação de entrega da coisa, o artigo 882.º do CC é o único relativo a esta obrigação. O n.º 1 deste

[205] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, p. 70; ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil VII – Direito das Obrigações, Contratos e negócios unilaterais*, 2ª reimpressão da 1ª ed. do tomo II da parte II de 2010, Almedina, 2016, p. 187.
[206] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, p. 73.
[207] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, pp. 82 a 84; JOSÉ ALBERTO VIEIRA, *Direitos Reais*, 2ª ed., Almedina, 2018, p. 220.
[208] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, p. 85.
[209] *Idem*, p. 93.

artigo destina-se a resolver os problemas resultantes do diferimento no tempo da obrigação de entrega da coisa. Não sendo a coisa entregue no momento de celebração do contrato, o seu estado pode variar até à altura da respetiva entrega. Na eventualidade de a coisa se deteriorar no período que medeia entre a realização do contrato e a sua efetiva entrega presume-se a responsabilidade do vendedor, segundo a regra geral de presunção de culpa do devedor estabelecida no artigo 799.º, n.º 1 do CC[210].

Conhecendo o estado da coisa que tem de ser entregue deve observar duas espécies de conduta: uma conduta negativa, a obrigação de se abster da prática de quaisquer atos que alterem o estado da coisa e, uma conduta positiva, a obrigação de fazer o necessário para a conservação da coisa no seu estado ao tempo da venda[211].Todos os aspetos relativos ao estado em que a coisa é entregue e a própria determinação do âmbito da obrigação de entrega encontram-se sujeitos ao princípio da autonomia das partes por força do artigo 405.º do CC[212].

A obrigação de entrega da coisa encontra-se subordinada às regras de cumprimento e incumprimento. Vale o disposto nos artigos 762.º e seguintes e 790.º do CC. Luís Menezes Leitão afirma que o cumprimento da obrigação de entrega da coisa opera a transmissão da respetiva posse para o comprador, se ele não for já possuidor. O problema está em saber se, por norma, a compra e venda não opera, mesmo sem a entrega, a transmissão da coisa por constituto possessório. Esta possibilidade é admitida por Luís Menezes Leitão, mas não como regra. Segundo este autor, é duvidoso se, após a venda, o vendedor não procede à entrega imediata da coisa, se deve presumir a verificação do constituto possessório, permanecendo o vendedor como detentor ou se se deve antes presumir a manutenção da posse no vendedor. Face à conceção objetivista da posse, Luís Menezes Leitão considera plasmada no artigo 1251.º do CC, a solução que entende o vendedor como possuidor em todas as hipóteses nas quais exerce poderes de facto sobre a coisa, apenas passando a detentor se for convencionado que passará a possuir em nome do comprador (artigo 1253.º, alínea c) do CC). Contudo, uma compreensão subjetivista da posse é dominante no entre nós[213].

[210] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019, pp. 107 e 108.
[211] *Idem*, p. 109.
[212] *Idem*, p. 111.
[213] *Idem*, pp. 112 e 113.

O terceiro e último dos efeitos essenciais da compra e venda é a obrigação de pagamento do preço, artigo 879.º, alínea c) do CC. Preço é por definição a expressão do valor em dinheiro. Contudo, uma coisa será a fixação do preço necessariamente em dinheiro e outra será a forma de pagamento em momento posterior à respetiva estipulação. O modo de realização cabe no âmbito da autonomia das partes[214].

Existem outros deveres pendentes sobre o comprador. Estes deveres podem ser classificados como não essenciais. Um desses deveres consiste e, salvo convenção ou usos em sentido contrário, na obrigação de o comprador suportar as despesas relativas à celebração do contrato nos termos do artigo 878.º do CC. Estas despesas são relativas simplesmente à celebração, recaindo as despesas relativamente à execução sobre o vendedor[215].

2. Podemos indicar desde já que, sendo o princípio da autonomia da vontade das partes um princípio essencial nesta matéria, fará todo o sentido a aplicação destas regras em sede de transmissão de criptoativos.

11.2. A transmissão da titularidade de criptoativos: MiCA vs. CC

1. As transmissões de criptoativos têm crescido exponencialmente e têm tido um enorme impacto no setor financeiro. Estas transmissões têm sido associadas a operações de branqueamento de capitais e de financiamento de terrorismo, atendendo à sua natureza transfronteiriça e à suscetibilidade de realização destas operações em anonimato[216].

Apesar de inicialmente os criptoativos terem surgido predominantemente como meio de pagamento, atualmente a realidade é diferente como é o caso da criptomoeda *ether,* que tem como principal funcionalidade suportar a rede *Ethereum,* ou a XRP, que tem como

[214] PEDRO DE ALBUQUERQUE, *Direito das Obrigações – Contratos em Especial I*, 2ª ed., Almedina, 2019p. 151.
[215] *Idem*, p. 165.
[216] MÁRCIA TOMÁS PIRES, "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, p. 194.

finalidade intermediar transações financeiras transnacionais de entidades bancárias e prestadores de serviços de pagamento[217].

Como já foi explorado em capítulos anteriores, o Regulamento MiCA visa primordialmente estabelecer regras específicas para as pessoas singulares e coletivas que prestam serviços relacionados com criptoativos de forma a proteger potenciais detentores não profissionais. Contudo, existem ainda questões a resolver no que diz respeito ao regime a aplicar na transmissão da titularidade dos criptoativos[218].

2. Os criptoativos podem ser titulados atendendo à sua capacidade transacional, ou seja, a capacidade prática de ocorrer uma transação na *blockchain*. Alguns autores defendiam que o proprietário de um criptoativo é quem tem a capacidade de gerar uma transferência em troca da qual o adquirente se encontra capaz de transferir uma contrapartida. Neste sentido, concluíam que era concebível o preenchimento de critérios como a transmissibilidade e a exigibilidade[219].

À primeira vista, a transmissão do criptoativo poderá ser vislumbrada como a transmissão da chave criptográfica privada, contudo não estaria correto uma vez que, da mesma forma que alguém quiser proceder à transferência de uma quantia bancária, não irá transmitir o código *pin* associado ao seu cartão multibanco como alerta MÁRCIA TOMÁS PIRES[220]. Tem de se entender por capacidade transacional, uma capacidade factual de ordenar determinada transmissão que altera a titularidade sob o criptoativo, existindo por base um conjunto de regras relativas às condições que se pretendem que a transação siga. A titularidade deveria assim estar subjacente à ordem dada para a realização da transação. Contudo, tal argumentação pode ser criticada pois uma conceção restrita neste âmbito teria como resultado a restrição do âmbito de objetos de titularidade, limitando-se a subsumir a titularidade a coisas tangíveis[221].

Uma vez que o titular do criptoativo perder acesso à chave criptográfica privada, também perderá a capacidade de efetuar transmissões com os criptoativos que se encontrem no

[217]MÁRCIA TOMÁS PIRES, "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, p. 194.
[218] *Idem*, p. 195.
[219] *Ibidem*.
[220] *Idem*, pp. 195 e 196.
[221] *Idem*, p. 196.

endereço público associado. Em matéria de registos podemos dizer que, os registos feitos em plataforma distribuída e descentralizada não são tidos como registos legalmente definitivos do título, não sendo comparáveis, por exemplo, ao registo predial. Tal significa que um terceiro, num cenário hipotético, poderá exercer controlo sobre o ativo se tiver acesso à chave privada[222].

Consideramos assim, como MÁRCIA TOMÁS PIRES, que a transmissão de criptoativos deve ser tratada como uma verdadeira re-transferência. Apesar da transmissão de A para B de um criptoativo ser considerada como uma nova saída, visa a representação do mesmo direito, em tudo igual ao criptoativo original[223].

3. Atendendo que a transmissão da titularidade tem como objeto o criptoativo em si, de forma a aferir qual o regime de transmissão aplicável nos termos do direito português, será necessário em primeiro lugar aferir qual é objeto da relação jurídica[224]. Nesta investigação, vamos apenas forcar-nos na transmissão de criptoativos que se encontram no âmbito da MiCA e deixar de parte a análise daqueles se encontram fora desse âmbito e são ainda regulados como valores mobiliários.

No que diz respeito a esta primeira categoria de criptoativos, podemos afirmar que estabelece o n.º 1 do artigo 202.º do CC que, por coisa, se consideram os objetos a respeito dos quais se podem transmitir direitos e obrigações por meio de negócios jurídicos. No parágrafo 5, n.º 1 do artigo 3.º do Regulamento MiCA estabelece como definição de criptoativos *"uma representação digital de um valor ou de um direito que pode ser transferida e armazenada eletronicamente, recorrendo à tecnologia de registo distribuído ou a uma tecnologia semelhante".* Com base nesta definição, podemos considerar os criptoativos coisas móveis fungíveis e incorpóreas nos termos do artigo 203.º do CC, podendo

[222] MÁRCIA TOMÁS PIRES, "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, p. 196.
[223] *Idem*, p. 197.
[224] *Idem*, p. 198 e 199.

ser objeto de negócios jurídicos[225]. Todos os negócios em torno dos mesmos se encontram, em regra geral, sujeitos à liberdade de forma, conforme estabelecido no artigo 219.º do CC.[226].

Com exceção dos NFTs, os criptoativos são tidos como coisas fungíveis nos termos do artigo 207.º do CC. Tal significa que são suscetíveis de ser substituídos quer pelo seu género, qualidade e quantidade.

A distinção entre coisas corpóreas e incorpóreas não consta do elenco do artigo 202.º, contudo essa distinção é feita pela doutrina para diferenciar coisas com base nas suas características. Como nos indica ANTÓNIO MENEZES CORDEIRO, a tradição greco-latina clássica define coisas incorpóreas como sendo as criações do espírito humano. Elas podem ser comunicadas através de linguagens e ser incorporadas em documento. As coisas incorpóreas compreendem três categorias: os bens intelectuais, as prestações e os *quid* jurídicos[227]. O *software* pode ser pensado nestes termos e inserido na categoria de bens intelectuais e, como vimos no caso de defeito da máquina, a programação também inclui os suportes materiais. Também as bases de dados, como a *blockchain,* concluímos nós, são vistas por este autor como inseridas no regime comum dos bens intelectuais[228].Tendo em conta que o criptoativo vive neste meio incorpóreo fará sentido que seja também considerado parte dele.

As características que se encontram predefinidas na *blockchain* tornam o controlo sob criptoativo funcionalmente similar ao controlo sob coisa móvel incorpórea, como temos vindo a determinar. Uma transferência de criptoativos, ainda que operacional na rede *blockchain*, é também similar à entrega da posse sob coisas móveis, em que o título é geralmente transferido quando exista intenção de transferir o título associado ao momento de entrega da posse. A regra geral deve ser que a titularidade sob criptoativo acompanha a transmissão que ocorre na confirmação da rede *blockchain*. O momento de transmissão

[225] MÁRCIA TOMÁS PIRES, "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, p. 198 e 199.
[226] *Idem*, p. 199.
[227] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil II – Parte Geral: Coisas*, 3ª ed., Almedina, pp. 158 e 159.
[228] *Idem*, pp. 155-168.

de criptoativos coincide com o momento da posse quando o criptoativo fica associado ao endereço público do adquirente[229].

Uma parte das transmissões de criptoativos ocorre no âmbito de contratos de compra e venda. A compra e venda é um negócio tido como suficiente para a transmissão da titularidade de criptoativos, não sendo necessário um negócio distinto para operar tal transferência. Atendendo ao princípio da autonomia privada das partes, nada obsta a que as partes determinem uma condição sob a qual a transação poderá ocorrer ou uma situação de reserva de propriedade nos termos gerias. A titularidade ocorrerá aquando da transferência efetiva para o endereço público da contraparte[230].

11.3. Regime aplicável no ordenamento português

1. Os criptoativos que se enquadram no âmbito material do Regulamento MiCA, tendo em conta a designação e características estipuladas no mesmo, inserem-se na classificação de coisas móveis fungíveis e incorpóreas para efeitos do ordenamento português. A transmissão destes bens deverá então ser feita pelo instrumento de excelência para tal operação, o contrato de compra e venda, através do qual, tendo em conta as características dos criptoativos, se transmitirá a propriedade sobre estes por mero efeito do contrato, tendo esse contrato as características que as partes desejarem.

O *smart contract*, tendo em conta o princípio de liberdade de forma no nosso direito contratual, poderá ser uma das formas adotadas para este tipo de transação.

[229] MÁRCIA TOMÁS PIRES, "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023, pp. 197 e 198.
[230] *Idem*, pp. 199 e 200.

12. QUESTÕES RELACIONADAS COM A TRANSMISSÃO DE CRIPTOATIVOS EM ESPECIAL O ENRIQUECIMENTO SEM CAUSA

1. No enriquecimento sem causa tradicional temos, de forma geral, uma deslocação patrimonial de uma esfera para outra ou, pelo menos, o radicar, numa esfera, de uma vantagem que, de acordo com os critérios comuns, deveria caber a outra[231]. Estamos perante uma fonte de obrigações genérica[232].

No exame dos requisitos gerais do enriquecimento sem causa, teremos de partir do artigo 473.º, n.º 1 do CC[233]. Sempre que se verifique o preenchimento de todos esses pressupostos, será possível interpor uma ação a exigir a restituição do enriquecimento sem causa[234]. Temos, à partida, um enriquecimento que traduz o ato e o efeito de obtenção de riqueza, isto é, de majorar da situação patrimonial já existente. Contudo, o enriquecimento não carece de apresentar um valor patrimonial. Tudo o que possa ser objeto de uma obrigação pode ser restituído: ou em si ou por equivalente – artigo 479.º, n.º 1. Logo pode ser transferido, criado ou majorado, dando azo a um enriquecimento[235].

De acordo com a tradição nacional, cumpre-se autonomizar, ao lado da ideia de enriquecimento, a ideia de empobrecimento. A individualização do "à custa de outrem" justifica esta interpretação. Pode-se falar em dano, aplicável ao enriquecimento sem causa, mas sem o confundir com o dano da responsabilidade civil. A não haver empobrecimento, o Direito não se preocuparia com o tema do enriquecimento[236].

---

[231] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, p. 206.
[232] LUÍS MENEZES LEITÃO, *Direito das Obrigações I – Introdução. Da constituição das obrigações*, 13ª ed., Almedina, 2016, p. 369.
[233] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, p. 223.
[234] LUÍS MENEZES LEITÃO, *Direito das Obrigações I – Introdução. Da constituição das obrigações*, 13ª ed., Almedina, 2016, p. 370.
[235] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, pp. 224 e 225.
[236] *Idem*, p. 227.

Entre o enriquecimento e o empobrecimento, deve existir uma relação. A jurisprudência alemã fez uma aplicação progressivamente mais lata. No limite, o requisito "à custa de outrem" acabaria mesmo por ser dispensável tanto no enriquecimento por prestação porque, por definição, a prestação tem um autor, sendo dispensável acrescentar que é "à custa dele", de acordo com CANARIS, e no enriquecimento por intervenção porque, estando em jogo o mero conteúdo da destinação, as vantagens do enriquecido não teriam de ocorrer à custa de ninguém, de acordo com REUTER/MARTINEK[237].

Trata-se de uma orientação de certo modo sufragada, entre nós, por MENEZES LEITÃO, quando considera que o empobrecimento nada mais seria do que a imputação do enriquecimento à esfera de outra pessoa. Considera este autor que o enriquecimento sem causa visaria reprimir o enriquecimento e não compensar o dano[238].

Como já indicámos, a lei emprega a expressão "enriquecer à custa de outrem" – art.º 473, n.º 1. Com base nessa locução, põe-se o tema de saber se a relação entre o enriquecido e o empobrecido deve ser direta ou se ela pode ser indireta, no sentido de o enriquecimento, em vez de transitar deste para aquele, poder ainda passar pela esfera de terceiros. Tradicionalmente, a doutrina entendia que "à custa de outrem" implicava imediação: o enriquecimento teria de passar, diretamente, do empobrecido para o enriquecido. Contra manifestou-se doutrina ulterior ao questionar o sentido da dita imediação. Esta replica outra doutrina: a ideia de imediação visa exprimir a ideia de que o enriquecimento, obtido à custa do empobrecido, deve chegar ao enriquecido, sem se perder por esferas de terceiros[239].

Podemos ter duas situações diferentes: a das alienações gratuitas do enriquecimento (artigos 289.º, n.º 2 e 481.º, n.º 1, a que poderemos somar o caso da pauliana (artigo 616.º, n.º 3) que, na prática, irá dar no mesmo: a lei desvaloriza o interesse do adquirente gratuito, conectando a sua vantagem ao empobrecido e a do pagamento de dívida de terceiro

[237] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, p. 230.
[238] LUÍS MENEZES LEITÃO, *Direito das Obrigações I – Introdução. Da constituição das obrigações*, 13ª ed., Almedina, 2016, p. 411.
[239] ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, p. 232.

de boa-fé, o que pode originar uma relação trilateral que o legislador português, na tradição da repetição do indevido, valorou a partir do credor[240].

Ainda é dúbio que o direito português aceite atribuições patrimoniais indiretas como enriquecimento pelo que fará mais sentido adotarmos a ideia da imediação como fator essencial no enriquecimento.

O artigo 473.º, n.º 1 exige, para o enriquecimento, que este tenha ocorrido "sem causa justificativa". Trata-se de um conceito, entre nós, considerado controvertido. As dificuldades prendem-se com o facto de fazer intervir toda a problemática ligada à unidade ou diversidade do enriquecimento e, ainda, a problemática do "à custa de" e a de colocar aqui o controverso tema da causa do contrato. Uma prestação não terá causa justificativa quando não advenha de nenhuma fonte ou de uma fonte válida, podendo ser hipótese de ausência de causa jurídica a inexistência da obrigação, o posterior desaparecimento da causa ou a não verificação do efeito pretendido (n.º 2)[241].

Desviamo-nos, assim, da afirmação segundo a qual a ausência de causa justificativa seria um conceito indeterminado. Semelhante asserção equivaleria a dizer que todas as transações que se fazem poderiam passar pelo crivo indeterminado de saber se teriam ou não causa justificativa. Na verdade, a causa é fundamentalmente a fonte. Assim, a falta de causa é a inaplicabilidade de uma norma que legitime a aquisição. Cada setor jurídico dirá, perante a concreta situação em jogo, se existe ou não, tal fonte de legitimação. Não compete ao enriquecimento sem causa, antecipando todo o ordenamento, explicar, caso a caso, quando é que certa atribuição tem cobertura jurídico-normativa. Não se confunde com a falta de causa justificativa a verificação das concretas condições exemplificadas no artigo 473.º, n.º 2[242].

Do enriquecimento resultante do artigo 473.º temos mais um requisito a considerar: a ideia de subsidiariedade. Esta subsidiariedade encontra-se consagrada no artigo 474.º que determina que a ação de enriquecimento sem causa não tem lugar quando a lei facultar ao

[240]ANTÓNIO MENEZES CORDEIRO, *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, 2016, Almedina, p. 233.
[241] *Idem*, pp. 235 e 237.
[242] *Idem*, p. 237 e 238.

empobrecido outro meio de ser indemnizado ou restituído, negar o direito à restituição e atribuir outros efeitos ao enriquecimento.

2. No contexto da *blockchain*, se a parte que deveria ter recolhido o benefício não for a pessoa que a ele tem direito, essa pessoa deverá ter o direito de pedir a restituição desse mesmo benefício sob a alçada do instituto do enriquecimento sem causa,[243]à semelhança do que acontece nos demais casos. Não vemos, assim, qualquer obstáculo ao preenchimento dos requisitos de enriquecimento, empobrecimento e causa justificativa no contexto de uma transação com criptoativos que preencha esses mesmos requisitos. A sua estrutura não impede, à partida, a verificação destes conceitos.

Perante um cenário de enriquecimento sem causa já foram apresentadas soluções nomeadamente por parte do *Coinbase* no que diz respeito ao *hard fork* da *Bitcoin Cash* em 2017. Em 2017, a *Bitcoin* foi alvo de um processo, o *hard fork*, já explorado nesta investigação, que levou à criação da *Bitcoin Cash*. Com base na natureza deste processo, todos os sujeitos que tinham *Bitcoin* antes ficaram com a mesma quantidade de *Bitcoin Cash* depois do processo. Por outro lado, os utilizadores de *Coinbase* foram inicialmente privados do acesso ao seu *Bitcoin Cash* e ameaçaram propor ações de enriquecimento sem causa. A questão foi resolvida sem a intervenção de um tribunal pelo que a incerteza legal desta questão persiste[244].

Para que alguém possa declarar enriquecimento sem causa, é necessário estabelecer o fator da falta de causa como já vimos. Determinar se uma causa é ou não injusta não é um exercício de discricionariedade, mas sim uma análise de fatores injustos reconhecidos. O outro elemento essencial no enriquecimento sem causa é a existência de um benefício. Um benefício pode ser tangível ou não tangível e pode ser qualquer coisa de valor, valor este determinado pela perspetiva do recipiente. Os benefícios podem ser considerados monetários ou não monetários, se disserem respeito a uma quantidade de dinheiro ou a

[243] JAZZ OSVALD, *Unjustly enriching the richer: a doctrinal analysis of unjust enrichment and its application to cryptocurrency hard fork and airdrop events*, Australian National University Journal of Law and Technology, 2020, p. 15.
[244] *Idem*, pp. 15 e 16.

um serviço respetivamente. Sendo um benefício monetário, este é considerado definitivamente benéfico[245].

O terceiro elemento, "à custa do empobrecido", não deve ser classificado como uma perda ou um ganho, mas sim como um benefício passado do empobrecido para o enriquecido. O que revela é a relação causal entre o ganho do enriquecido e a injustiça perante o empobrecido. Normalmente o foco está no benefício inicial, como o dinheiro enviado acidentalmente a outra pessoa e não para aquela a que o dinheiro era destinado. Contudo, sendo o dinheiro inicialmente transferido utilizado para criar lucro, a restituição deverá incluir também este lucro[246].

À partida, não parecem existir obstáculos de maior à aplicação deste regime aos *smart contracts*, mas iremos analisar agora um caso de possível enriquecimento sem causa envolvendo criptoativos.

3. O caso THEODORE RIDER VS. UPHOLD[247] foi um caso que analisou a possibilidade de aplicação deste instituto no mundo da *blockchain*. São feitas acusações de negligência, negligência grosseira, violação do contrato, violação de normas e enriquecimento sem causa, contudo iremos focar-nos mais no debate inicial relativo à natureza dos criptoativos e de instituições como a Uphold e claro a questão do enriquecimento sem causa.

A Uphold era uma plataforma de troca de criptoativos que permitia aos seus utilizadores transferir, comprar, trocar, reter e transacionar criptoativos. Para criarem uma conta, os utilizadores tinham de definir uma autenticação de dois fatores e tal mecanismo requeria o uso de um servidor de autenticação que enviava um código único para o dispositivo que o utilizador indicou.

Os autores eram uma classe de utilizadores atuais e antigos cujas contas foram acedidas por indivíduos não autorizados. Estes consideraram que a autenticação em dois fatores

[245] JAZZ OSVALD, *Unjustly enriching the richer: a doctrinal analysis of unjust enrichment and its application to cryptocurrency hard fork and airdrop events*, Australian National University Journal of Law and Technology, 2020, pp. 25 e 26.
[246] *Idem*, pp. 28 e 29.
[247] THEODORE RIDER, et al., -v- UPHOLD HQ INC., et al., United States District Court Southern District of New York, 22 de fevereiro de 2023.

falhou, o que permitiu a utilizadores não autorizados a possibilidade de designar novos dispositivos, empregando o *e-mail* e *password* dos utilizadores da plataforma. Os autores indicaram também os réus deram a entender que os protocolos de segurança estavam de acordo com as regras em vigor e que haveria uma monotorização do estado das contas, alertando para qualquer possível falha de segurança. Tal levou a que os autores perdessem os seus criptoativos e informação pessoal e financeira que constava das suas contas.

Em primeiro lugar, é analisado o EFTA, defendendo a Uphold que este não poderá ter sido violado porque este se aplica a transferências de fundos e os criptoativos não podem ser considerados fundos para este efeito. Para efeitos deste ato, uma transferência eletrónica de fundos refere-se a uma transação originada por cheque ou instrumento de papel semelhante que é iniciada num terminal eletrónico para instruir ou autorizar uma instituição financeira a creditar ou debitar uma conta. Aqui a instituição financeira pode ser definida como o Estado ou um banco nacional, uma associação de empréstimos e poupanças ao nível estadual ou federal, uniões de crédito estaduais ou federais, ou qualquer pessoa que, direta ou indiretamente, tenha em posse uma conta que pertença a um consumidor.

A Uphold parece enquadrar-se na definição de instituição financeira, numa interpretação meramente literal do artigo, deste ato, tendo em conta que mantém contas na sua plataforma de criptoativos e também parecia realizar estas transferências eletrónicas de fundos. A dúvida estaria em determinar se os criptoativos poderiam ser considerados fundos. Não havendo uma definição no ato, o tribunal considerou que, havendo termo indeterminado, os tribunais deveriam dar ao termo o seu significado comum.

O tribunal considerou que o termo *"fundos"* diria respeito a uma quantidade de dinheiro ou outros estabelecido com um propósito específico. Os criptoativos, naquela altura, eram considerados moeda digital ou virtual, emitida por uma entidade descentralizada que funcionava como meio de pagamento, usa tecnologia encriptada para regular a geração de mais unidades de criptomoeda, verificava transferências e prevenia fraudes. Este considerou que o seu significado comum seria uma forma digital de ativos monetários e líquidos que constituem fundos para efeitos do EFTA. O tribunal alertou também para o facto de o estatuto contra o branqueamento de capitais, no seu termo de fundos, não ter discriminado o tipo de moeda, apenas que ela possa ser usada para pagar coisas.

A posição dos réus para defender a não inclusão dos criptoativos na categoria de fundos partiu de uma declaração do CFPB que determinava que não haveria lugar à aplicação de estatutos já existentes, como o EFTA, a serviços e moedas virtuais e que ainda estava a proceder à análise deste tipo de moedas virtuais. Com base nesta declaração, o tribunal concluiu pela procedência deste argumento dos réus para afastar a classificação dos criptoativos como fundos para este efeito.

Os autores defendem a verificação de um caso de enriquecimento sem causa. De acordo com a lei de Nova Iorque, para tal o autor deverá alegar que os réus foram beneficiados, que foram beneficiados à custa dos autores e que a equidade e boa-fé requerem a restituição. O tribunal afirma que esta justificação não pode ser utilizada quando todas as outras falham. Não está disponível se for apenas uma forma de duplicar ou substituir um contrato como tem sido feito ao longo da ação. Uma acusação típica de enriquecimento sem causa envolveria um réu que, sem culpa, teria recebido dinheiro ou qualquer vantagem à qual não tivesse direito. Novamente, os autores não fazem uma distinção entre a acusação de violação de cláusulas contratuais e esta acusação. Os autores defendem que a Uphold beneficiou das taxas de transação pagas por eles e que seria injusto deixar que a Uphold ficasse com o lucro por manter medidas de proteção de dados inadequadas. Tendo em conta estes aspetos, o tribunal ignora esta acusação por ser duplicativa por utilizar os mesmos argumentos que utilizou para justificar a violação contratual.

A conclusão do tribunal foi de não provimento das acusações feitas pelos autores.

4. Consideramos que a possibilidade abstrata deste regime ser aplicável aos criptoativos não é afetada pelo que foi dito nesta decisão pois neste caso os autores não tinham argumentos suficientes fortes para defender o enriquecimento e outras transgressões. Esta exposição servirá apenas para demonstrar a possibilidade de demanda por enriquecimento sem causa no contexto de uma transação de criptoativos. Contudo, estamos perante um caso regulado pelo direito norte-americano, bastante diferente do nosso direito. Sem prejuízo da verificação dos mesmos pressupostos, teremos de atender à ideia da subsidiariedade consagrada no nosso direito.

O anonimato continua a constituir, à primeira vista, um obstáculo para a aplicação deste instituto pois, sendo ele verificável nos casos em que a subsidiariedade o permita, teremos

de analisar como se deverá proceder à notificação daquele que se viu enriquecido sem causa justificativa.

13. CONCLUSÕES

1. Ao longo desta investigação, procurámos responder a seis questões que se centravam na ideia de transmissão de criptoativos.

2. Numa perspetiva histórica procedemos à análise das soluções do regime português em matéria de criptoativos. Contudo, com o aparecimento do Regulamento MiCA a nível europeu, essas soluções deixaram de ter relevância, tendo em conta a hierarquia de regulamentação que existe no nosso ordenamento. Uma vez analisado o regime da MiCA, deparamo-nos com uma lacuna ao nível da transmissão destes ativos, da moldura contratual por detrás desta e todas as consequências que podem advir dessa transmissão.

Temos regras relativas às ofertas públicas e à colocação à negociação dos criptoativos em plataformas de criptoativos, mas nada que nos auxilie na determinação de um sistema alternativo em matéria de transmissão, incumprimento, etc. Parece-nos assim que a determinação desse regime tenha sido deixada à autonomia de cada Estado-membro, consoante as suas regras de direito civil.

3. De forma a percebermos se os *smart contracts* seriam uma forma eficaz de fazer operar estas transações, analisámos em primeiro lugar a viabilidade destes instrumentos que, apesar de apresentarem tanto vantagens e como desvantagens aos níveis legal e económico, parecem-nos um meio adequado para realizar a transmissão de criptoativos. Podemos considerar assim os *smart contracts* uma forma especial de contratar que poderá ser equiparada ao contrato por força dos princípios de liberdade de forma e de autonomia das partes.

De seguida, procedemos a uma análise dos aspetos específicos do direito contratual de forma a determinar se haveria semelhanças significativas entre os contratos tradicionais e os *smart contracts*. Por um lado, constatámos semelhanças em especial ao nível da formação do contrato. Por outro, encontrámos diferenças flagrantes nomeadamente por força da imutabilidade para efeitos de modificação e cessação do contrato. Estas diferenças partem da estrutura específica dos *smart contracts,* pelo que apenas devem ser aplicáveis a estes os institutos de direito civil cujos requisitos este novo tipo de tecnologia possa

preencher. A discriminação de regras específicas de resolução de problemas pelo próprio contrato será sempre privilegiada, especialmente num momento em que as redes de *blockchain* não possuem sistemas próprios de resolução de litígios.

4. A aplicação do direito português ou de qualquer direito nacional depende do funcionamento das normas de conflito em matéria de obrigações contratuais e extracontratuais. Estas obrigações encontram-se no âmbito de aplicação material dos Regulamentos europeus Roma I e II respetivamente.

5. Sendo possível a aplicação do direito português nesta sede, tanto por escolha das partes, como por aplicação dos artigos que determinam o direito na falta de escolha, fez todo o sentido analisar as normas de direito português relativamente ao instituto da compra e venda para determinar a possibilidade de transação de criptoativos nesta sede. Decidimos que as características dos criptoativos não chocavam com a aplicação do regime dos contratos de compra e venda pelo que cabe aqui a aplicação do mesmo no contexto da transmissão de criptoativos. Estes criptoativos poderão ser enquadrados nas já existentes classificações de coisa, na estrutura do contrato de compra e venda e na ideia de propriedade e titularidade.

6. Analisámos separadamente a matéria de enriquecimento sem causa por ser um instituto extracontratual. Parece-nos ser possível aplicar todos os requisitos do instituto do enriquecimento sem causa quando sucedam no meio dos criptoativos. Quando ocorra um problema na transação, o anonimato e privacidade são características importantes no contexto da *blockchain*. Contudo, em caso de enriquecimento sem causa, podemos contornar o anonimato tendo em conta a não impossibilidade de determinação da identidade dos sujeitos que contratam.

7. Apesar da natureza descentralizada da *blockchain*, fará sentido que seja possível, quando regras fulcrais sobre interpretação, incumprimento, modificação, entre outras não constem do clausulado, aplicar o direito dos Estados, em especial o direito contratual português. A aplicação do direito nacional deve servir como uma forma de garantir a segurança dos intervenientes quando estes pretendam transmitir criptoativos entre eles. Contudo, teremos de ter sempre em atenção os contornos específicos dos *smart contracts*

e o facto de estes não serem flexíveis de uma maneira geral. Haverá aplicação dos institutos gerais quando seja manifestamente necessário e não existam regras no contrato atinentes a determinado tópico.

14. BIBLIOGRAFIA

AKKA, LAWRENCE / GOODMAN, SAM / LAVY, MATTHEW ET. AL – *Legal Statement on Cryptoassets and Smart Contracts*, UK Jurisdiction Taskforce, disponível em https://technation.io/about-us/lawtech-panel, 2019.

ALBUQUERQUE, PEDRO DE – *Direito das Obrigações - Contratos em Especial I*, 2ª ed., Almedina, 2023.

ALHARBY, MAHER / MOORSEL, AAD VAN – *Blockchain-based Smart Contracts: A Systematic Mapping Study*, 2017.

ALVES, HUGO RAMOS – "Smart Contracts: Entre a Tradição e a Inovação" em *Fintech II – Novos Estudos sobre a Tecnologia Financeira*, António Menezes Cordeiro, Ana Perestrelo de Oliveira e Diogo Pereira Duarte (coord.), Almedina, 2019.

ATZORI, MARCELLA – *Blockchain Technology and Decentralized Governance: Is the State Still Necessary*, 2015.

BABICEAN, ANDREEA – *Blockchain e Regulação: Perspetivas de uma Regulação de Valores Mobiliários sob a forma de Criptoativos*, Almedina, 2024.

BHUSHAN, BHARAT / GUPTA, SAHIL / SINHA, SHUBHAM – *Emergence of Blockchain Technology: Fundamentals, Working and its Various Implementations*, International Conference on Innovative Computing and Communication, 2020.

BUTERIN, VITALIK / ILLUM, JACOB / NADLER, MATTHIAS, EL. AL. – *Blockchain Privacy and Regulatory Compliance Towards a Practical Equilibrium*, disponível em https://ssrn.com/abstract=4563364, 2023.

CÂMARA, PAULO – *Manual de Direito dos Valores Mobiliários*, 4ªedição, Almedina, 2018.

CANNARSA, MICHEL / DIMATTEO, LARRY A. / PONCIBÒ, CRISTINA – "Smart Contracts and Contract Law" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019.

CARIA, RICCARDO DE – "Definitions of Smart Contracts: Between Law and Code", em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019.

CATALINI, CHRISTIAN / GANS, JOSHUA S. – *Some Simple Economics of the Blockchain*, Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16, disponível em https://ssrn.com/abstract=2874598, 2022.

CHOHAN, USAMAN W. – *A History of Bitcoin*, Notes of the 21st century, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047875, 2022.

CHOHAN, USAMAN W. – *Crypocurrencies: A Brief Thematic Review*, Notes on the 21st century, disponível em https://ssrn.com/abstract=3024330, 2022.

CORDEIRO, ANTÓNIO MENEZES – *Tratado de Direito Civil II – Parte Geral – Negócio Jurídico*, 5ª ed., Almedina, 2023.

CORDEIRO, ANTÓNIO MENEZES – *Tratado de Direito Civil II – Parte Geral – Coisas*, 3ª ed., Almedina, 2013.

CORDEIRO, ANTÓNIO MENEZES – *Tratado de Direito Civil VIII – Direito das Obrigações, Gestão de negócios, enriquecimento sem causa, responsabilidade civil*, 2ª Reimpressão da 1ª ed. do tomo III da parte II de 2010, Almedina, 2016.

CORDEIRO, ANTÓNIO MENEZES – *Tratado de Direito Civil IX – Direito das Obrigações, Cumprimento e não cumprimento: transmissão, modificação e extinção*, 2ª ed. revista e aumentada, Almedina, 2016.

CORDEIRO, ANTÓNIO MENEZES – *Tratado de Direito Civil XI – Contratos em especial (1ª parte), compra e venda; doação; sociedade; locação*, Reimpressão, Almedina, 2019.

CONG, LIN WILLIAM / HE, ZHIGUO – *Blockchain Disruption and Smart Contracts*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764, 2023.

CORNELL, NICOLAS / WERBACH, KEVIN – *Contracts Ex Machina*, Duke Law Journal, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2936294, 2017.

CRAVO, LAURA ABREU – "Regulação dos Criptoativos na Era Pré MiCA", em *MiCA: Estudos sobre a Nova Regulação Europeia de Criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (coord.), Almedina, 2023.

DE FILIPPI, PRIMAVERA / WRIGHT, AARON – *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664, 2015, revisto em 2017.

DUROVIC, MANTEJA / JANSSEN, ANDRÉ – *The Formation of Blockchain-based Smart Contracts in the Light of Contract Law*, European Review of Private Law 6, disponível em https://www.semanticscholar.org/paper/The-Formation-of-Blockchain-based-Smart-Contracts-Janssen-Durovic/d2b8aedf3ceae1f244f3578fc05c78d3a55996a0, 2019.

DUROVIC, MATEJA / JANSSEN, ANDRÉ – *The Formation of Smart contracts and Beyond: Shaking the Fundamentals of Contract Law*, versão alargada do artigo anterior.

JACCARD, GABRIEL OLIVIER BENJAMIN – *Smart contracts and the role of Law*, Jusletter IT 23, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099885, 2017.

JENA, DEBASISH, MOHANTA / BHABENDU KUMAR / PANDA, SOUMYASHEE S. – *An Overview of Smart Contract and Use Cases in Blockchain Technology*, 2018.

JUELS, ARI / MARINO, BILL – *Setting Standards for Altering and Undoing Smart Contracts*, Springer International Publishing Switzerland, 2016.

KHAN, SHAFAQ NAHEED / LOUKIL, FAIZA / GHEDIRA-GUEGAN, ET. AL. – *Blockchain smart contracts: Applications, challenges and future trends*, Peer-to-Peer Networking and Applications, 2021.

KOLVART, MARGUS POOLA / MERIT, ADDI RULL – *Smart Contracts*, Springer International Publishing Switzerland, 2016.

LAUSHTI, KRISTIAN / MATTILA, JURI / SEPALLA, TIMO – *Smart Contracts – How Will Blockchain Technology Affect Contractual Practices?*, ETLA Reports no. 68, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3154043, 2018.

LEITÃO, LUÍS MANUEL TELES DE – *Direito das Obrigações I – Introdução. Da constituição das obrigações*, 13ª ed., Almedina, 2016.

LEITÃO, LUÍS MANUEL TELES DE – *Direito das Obrigações II - Transmissão e Extinção das Obrigações; Não Cumprimento e Garantias de Crédito*, 13ª ed., Almedina, 2023.

LEITÃO, LUÍS MANUEL TELES DE – *Direito das Obrigações III – Contratos em especial*, 14ª ed., Almedina, 2022.

MIK, ELIZA – "Blockchains – A Technology for Decentralized Marketplaces" em *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms*, disponível em https://doi.org/10.1017/9781108592239, 2019.

NAKAMOTO, SATOSHI – *Bitcoin: A Peer-to-Peer Electronic Cash System*, disponível em https://bitcoin.org/bitcoin.pdf, 2008.

OSVALD, JAZZ – *Unjustly enriching the richer: a doctrinal analysis of unjust enrichment and its application to cryptocurrency hard fork and airdrop events*, Australian National University Journal of Law and Technology, 2020.

PERESTRELO, ANA DE OLIVEIRA – *Smart Contracts, Risco e Codificação da Desvinculação ou Modificação negocial: Os falsos dilemas da Inter-relação Lei-código nos contratos empresariais*, Almedina, 2023.

PINHEIRO, LUÍS DE LIMA – *Direito Internacional Privado I – Introdução e Direito de Conflitos, Parte Geral*, 3ª ed. refundida, AAFDL Editora, 2019.

PILKINGTON, MARC – *Blockchain Technology: Principles and Applications*, Research Handbook on Digital Transformations, disponível em https://ssrn.com/abstract=2662660, 2016.

PIRES, MÁRCIA TOMÁS – "A transmissão da titularidade de criptoativos no ordenamento jurídico português: aspetos jurídicos e implicações práticas no regulamento mica" em *MiCA: Estudos sobre a nova regulação de criptoativos*, João Vieira dos Santos, João Luz Soares, Martinho Lucas Pires e Guilherme Maia (Coord.), Almedina, 2023.

RASKIN, MAX – *The Law and Legality of Smart Contracts*, Georgetown Law

Techonology Review, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959166, 2017.

ROHR, JONATHAN / WRIGHT, AARON – *Blockchain-Based Token Sales, Initial Coin Offerings and the Democratization of Public Capital Markets*, University of Tennessee Legal Studies Research Paper No. 338, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3048104, 2017, revisto em 2023.

ROLO, ANTÓNIO GARCIA – *Criptoativo – conceito, modalidades, regime e distinção de figuras afins*, Centro de Investigação de Direito Privado, revista nº 18/2022, disponível em https://ssrn.com/abstract=412358, 2022.

SANTOS, JOÃO VIEIRA DOS – "Regulação dos Criptoativos" em *Cadernos do Mercado de*

Valores Mobiliários, disponível em https://ssrn.com/abstract=3793662, 2021.

SBAZO, NICK – *Smart contracts*, disponível em https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html, 1994.

SCHAR, FABIAN – *Decentralized Finance: On Blockchain and Smart Contract-based Financial Markets*, Federal Reserve Bank of St. Louis Review, disponível em https://ssrn.com/abstract=3843844, 2021.

TRAUTMAN, LAWRENCE J. – *Is Disruptive Blockchain Technology the Future of Financial Services?*, Quarterly Report, disponível em https://ssrn.com/abstract=2786186.

VERSTRAETE, MARK – *The Stakes of Smart Contracts*, 50 Loyola University Chicago Law Journal 743, Arizona Legal Studies Discussion Paper No. 18-20, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3178393, 2018, revisto em 2019.

VIEIRA, JOSÉ ALBERTO – *Direitos Reais*, 2ª ed., Almedina, 2018.

WITTE, J. H. – *The Blockchain: a Gentle Introduction*, Record Currency Management,

Windsor, UK, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2887567, 2016.

Z. ZHENG, S. XIE, H.-N. DAI ET AL., *An overview on smart contracts: Challenges, advances and platforms*, *Future Generation Computer Systems*, disponível em https://doi.org/10.1016/j.future.2019.12.019., 2019.

15. JURISPRUDÊNCIA

SKATTEVERKET -v- DAVID HEDQVIST, Tribunal de Justiça da União Europeia, processo C 264/14, 22 de outubro de 2015, disponível em http://curia.europa.eu/.

THEODORE RIDER, et al., -v- UPHOLD HQ INC., et al., United States District Court Southern District of New York, 22 de fevereiro de 2023.