SMART CONTRACTS

Smart Contracts

Os smart contracts - códigos de programação de computador que permitem, por operação do próprio computador, monitorizar e/ou executar contratos, sem necessidade de interferência humana - já são uma realidade. Embora a sua utilização ainda não esteja generalizada, os desenvolvimentos que se têm verificado na utilização de blockchains fazem antever um grande leque de utilizações inovadoras.
Este cenário promissor coloca, contudo, algumas interrogações no plano jurídico, que resultam, sobretudo, do estado embrionário de desenvolvimento desta tecnologia. Por forma a garantir a tutela das partes envolvidas, é importante que o Direito acompanhe de perto a evolução dos smart contracts e das blockchains por estes utilizadas, promovendo assim o desenvolvimento juridicamente sustentado desta tecnologia.

Smart Contracts

Smart contracts - computer codes used for monitoring and performing contractual terms without human interference - have become real. Although its deployment is not widespread, the recent developments in blockchain technology promises to open up a wide array of innovative possibilities.
This promising scenario raises some question marks which result, in particular, from the embryonic status of development of this technology. In order to safeguard the position of the parties involved, it is important that the Law monitors the evolution of smart contracts and of the blockchains used by the latter, thereby promoting the legally sustained development of this technology.

Palavras chave
Processo Smart Contracts, Blockchain, Códigos de Programação, Tecnologia de Registo Descentralizado, Contratos de Execução Automática.

Key words
Smart Contracts, Blockchain, Programming Codes, Distributed Edger Technology, Self-Executing Contracts.

Fecha de recepción: 15-4-2017 *Fecha de aceptación: 29-5-2017*

INTRODUÇÃO AOS *SMART CONTRACTS*

O que são?

O conceito de *smart contract* não é novo. Foi inventado pelo criptógrafo Nick Szabo em 1994, mas só agora começa a ganhar relevância no léxico da criptografia, das tecnologias de informação e, por razões que a própria terminologia faz antecipar, dos juristas.

Por definição, um *smart contract* é um código de programação de computador que permite, por operação do próprio computador, monitorizar e/ou executar um contrato, sem necessidade de interferência humana.

Nesses códigos de programação, são definidas regras e consequências estritas para determinados eventos que o computador pode verificar, estabelecendo as obrigações, os benefícios e as penalidades aplicáveis, e procedendo à respetiva execução.

Importa notar em todo o caso que, como os *smart contracts* funcionam com programas de computador, é essencial que as obrigações, benefícios e penalidades aí previstos, e o modo e tempo de tomada de cada ação, estejam definidos de forma clara e verificável pelo computador. Com efeito, não tendo o computador inteligência humana, não tem a capacidade de abstração necessária para fazer juízos interpretativos ou solucionar ambiguidades linguísticas típicas dos contratos. Por conseguinte, os *smarts contracts* respeitam somente a contratos, ou conjuntos de cláusulas de um determinado contrato, que possa ser automatizado pelas partes em termos que apliquem a seguinte fórmula: «*Se ocorrer o evento X, então o código de computador desencadeará a consequência Y*».

Para que a fórmula acima referida possa ser aplicada, é essencial que o computador tenha meios para (a) detetar a ocorrência do evento X, e (b) fazer executar a consequência Y.

Como funcionam?

Através da fórmula acima descrita, os *smart contracts* podem desempenhar um inúmero conjunto de utilidades, de que são exemplo (i) a transferência automática de instrumentos financeiros após a receção de fundos, ou (ii) o pagamento de determinados montantes de capital e juros, em determinadas datas ou mediante a verificação de determinadas condições. Trata-se somente de um exemplo, pois na verdade os *smart contracts* podem aplicar-se a toda e qualquer circunstância em que um computador possa detetar a existência de um determinado evento e acionar uma consequência pré-definida.

Porém, como o computador apenas pode efetuar operações no domínio virtual, as ações que envolvam uma prestação material, como seja o caso do fornecimento de bens e serviços - v.g. a entrega de um livro ou a prestação de serviços de limpeza - continuarão necessariamente a ser cumpridas manualmente.

A UTILIZAÇÃO DE BLOCKCHAINS

Os *smart contracts*, enquanto código programação informática, eram já concebíveis desde que surgiu o computador. O que atualmente propulsiona a sua ascensão são as possibilidades abertas pela sua integração e execução no que comummente se chama de «*blockchain*» ou, de forma mais genérica, «*distributed ledger technology*».

Assim, para que o modelo de *smart contracts* funcione, os códigos dos *smart contracts* não são guardados pelas partes, sendo ao invés encriptados e enviados para outros computadores através de uma rede, a *blockchain*. Como veremos de seguida, as *blockchains* desempenham um papel essencial para a utilização de *smart contracts*.

As *blockchains* são bancos de dados, que funcionam como livro de registo de informações que a ela são trazidas por cada um dos computadores que a elas se encontra ligado (*distributed ledger*).

Cada nova informação que é trazida para a *blockchain* - por exemplo, um novo *smart contract* acordado entre duas partes - constitui um bloco, que se liga aos restantes blocos constituintes da *blockchain*.

Cada um dos computadores integrantes de uma rede é denominado «nó». Cada nó ajuda a distribuir cópias atualizadas em tempo real da cadeia de blocos em uso na *blockchain*. Cada vez que transações são realizadas, e portanto, são adicionados novos blocos, estas transações são comunicadas a todos os nós, para que possam atualizar os registos com as novas informações. Uma determinada transação apenas se considerará incluída na *blockchain* quando todos os computadores que a integrem tenham atualizado a respetiva base de dados.

Em resultado do processo de atualização simultânea de todos os nós da *blockchain*, o conjunto de informação detida a cada momento por cada nó integrante de uma determinada *blockchain* é exatamente o mesmo.

Para certificar uma informação numa cadeia de blocos e evitar fraudes, a *blockchain* conta com um mecanismo chamado *proof of work*, que corresponde a um protocolo criptográfico que valida uma transação num computador por meio da resolução de um problema matemático.

Adulterações nas cadeias de blocos, por menores que sejam, gerarão resultados diferentes do esperado para esse problema matemático. Tal circunstância impedirá o processamento da transação e, consequentemente, o seu registo pelos nós que compõem a *blockchain*.

Esta estrutura permite assim assegurar que, quando todos os computadores de uma determinada *blockchain* atualizem a respetiva base de dados com uma nova operação, essa operação se considere fidedigna, por ter sido aprovada por todos os nós da *blockchain*.

O propósito deste tipo de estrutura é minimizar o risco de manipulação por uma das partes num *smart contract*, pois a partir do momento em que o *smart contract* é incluído no sistema, torna-se insuscetível de alteração ou atualização unilateral por uma das partes.

A grande vantagem deste sistema face a uma alternativa de registo central, é a mitigação do risco de corrupção do registo central por uma das partes no *smart contract*, que terá, neste caso, a tarefa de corromper todos os computadores do sistema para poder unilateralmente alterar, ou suspender a execução, de um *smart contract* que tenha celebrado com um terceiro.

A este respeito, observa-se que a utilização de *blockchains* tornou-se conhecida por ser a tecnologia subjacente ao *bitcoin*, a moeda virtual mais utilizada *online*. A possibilidade de executar *smart contracts* complexos naquela *blockchain* - algo que se aponta como possível ainda este ano - tornaria possível a transferência de automática de fundos ao abrigo de um *smart contracts*.

Um aspeto adicional a destacar nesta sede é a transparência do sistema: as transações são divulgadas a todos os membros da *blockchain*, o que significa que todos os participantes podem controlá-las. Os mecanismos de criptografia fazem com que os usuários do sistema não necessitem de ser identificados.

Há, em todo o caso, desafios que se colocam nesta sede, como seja a conformidade das *blockchains* com as leis de proteção de dados pessoais, que

podem atribuir aos usuários o direito de exigir a eliminação dos seus dados, em contraposição com a regra de imutabilidade dos blocos de uma *blockchain*. Soluções para estes problemas estão a ser ensaiadas como, por exemplo, a possibilidade de restringir a visibilidade de certas informações a todos os participantes da *blockchain*.

SMART CONTRACTS - QUALIFICAÇÃO COMO CONTRATO?

Não obstante o exoterismo que lhes é emprestado pela terminologia dominante, os *smart contracts* não serão um corpo assim tão estranho ao sistema jurídico. Aliás, os constrangimentos à sua utilização resultarão mais de fatores tecnológicos e comerciais do que jurídicos, salvaguardando, claro, o impacto do quadro regulatório aplicável.

Como se referiu, muitas das dificuldades colocadas por estes contratos não são novas, tendo surgido no passado a propósito, designadamente, das máquinas de vendas automáticas (as denominadas máquinas de «*vending*») e, mais recentemente, da negociação algorítmica.

Tal não significa, contudo, que os sistemas jurídicos não possam ou não tenham mesmo de evoluir de forma a proporcionar soluções mais adaptadas às novas necessidades, sendo preciso atender às especificidades de cada caso, ponderando as concretas circunstâncias tecnológicas e comerciais. Alguns aspetos concretos ajudam a evidenciar estas afirmações.

Desde logo, num plano conceptual, o que aqui se entende por *smart contract* é reconduzível, pelo menos parcialmente, ao conceito de contrato: trata-se de um acordo assente na vontade simultaneamente confluente manifestada por duas ou mais entidades (que agiram por si ou através de representante) e que produz efeitos jurídicos.

O *smart contract* pode corresponder ao contrato em si mesmo, i.e. as partes celebram um acordo que está materializado em códigos de computador, ou simplesmente reportar-se a uma ou mais cláusulas de um contrato escrito ou verbal, que passa assim a ser executado, quanto a essas cláusulas específicas, através de um código de computador.

Quanto à forma, onde vigore o princípio da liberdade de forma, não se vê obstáculos a que os contratos sejam celebrados e representados por código informático numa *blockchain*, o que, aliás, muito se assemelha ao que sucede atualmente em alguns espaços, nomeadamente no que diz respeito a derivados negociados em mercado regulamentado. Contudo, nada obsta a que o recurso a programas informáticos executados em *blockchains* seja ele próprio objeto de um contrato dito convencional, reduzido ou não a escrito, que regule os termos em que esses programas informáticos serão utilizados. A utilização de *blockchains* poderá assim ser objeto de uma contratação-quadro convencional, que estabelece, em termos obrigacionais, ou mesmo reais, como funcionarão os *smart contracts* e como é que as partes e a situação dos bens em causa serão afetadas juridicamente pelo resultado da «execução» do código a que se chama *smart contract*.

Por seu turno, é sobre a «execução» que poderão residir as maiores dúvidas. Nos escritos sobre *smart contracts*, cuja proveniência varia das tecnologias de informação ao Direito, é comum afirmar-se que uma das características mais disruptivas (incluindo do ponto de vista jurídico) dos *smart contracts* é serem «*self-enforceable*» ou «*self-executing*», chegando-se mesmo a afirmar que deixariam de ser necessários tribunais.

Todavia, em face das coordenadas jurídicas atuais, é necessário traçar uma linha entre execução do contrato (no sentido de cumprimento das prestações que são devidas) e o recurso a mecanismos heterónomos de resolução de litígios (*enforceability*). A capacidade de auto-execução dos *smart contracts* não deve ser confundida com a possibilidade de se recorrer a um tribunal para, por exemplo, pedir a restituição de um determinado montante que foi transferido para a esfera da contraparte por erro do código informático ou pedir a declaração de nulidade do contrato.

ASPETOS REGULATÓRIOS - *SMART CONTRACTS* FINANCEIROS

Olhando para o quadro regulatório nacional e europeu dos mercados financeiros, constata-se que não existem regras que visem especificamente a utilização de *smart contracts* nos mercados financeiros, setor onde o surto de utilização dos *smart contracts* é mais esperado.

Atendendo ao seu estado embrionário, não é possível prever com segurança qual será a evolução do quadro regulatório aplicável ao desenvolvimento e comercialização de produtos financeiros que neles se baseiem. Além do mais, esse quadro será indis-

sociável do tratamento e reconhecimento reservado às *blockchains*, o que, em última instância, poderá ditar uma refundação das estruturas do mercado, com alterações substanciais dos papéis e responsabilidades dos agentes que existem atualmente: o que a ESMA denomina de «*New Model*» (European Securitites and Markets Authority, Report: The Distributed Ledger Technology Applied to Securities Markets, «*ESMA Report*», pág 29, disponível em https://www.esma.europa.eu/file/21298/download?token=L3KmGxpA).

Por outro lado, apesar de os *smart contracts* ainda não terem sido utilizados em larga escala, as potencialidades e o investimento reunido à sua volta justificam as interrogações quanto ao seu enquadramento regulatório. Estas incertezas acentuam-se em espaços com grande densidade regulatória, como é o caso dos mercados financeiros, sendo que, no curto-prazo, o mais provável é que a utilização de *smart contracts* nos mercados financeiros tenha de conviver e ser enquadrada no quadro regulatório vigente.

Nesse mesmo curto-prazo, o cenário mais plausível é o da utilização das *blockchains* de forma segmentada, como forma de tornar mais eficientes alguns processos «tradicionais» dos mercados, ao invés de operar uma revolução das suas estruturas: ou seja, um modelo de otimização («*Optimised Model*», na terminologia da ESMA, *ESMA Report*).

Em geral, é no campo das atividades *post-trading* (v.g., compensação e liquidação) que se prevê que as *blockchains* sejam inicialmente introduzidas. Em particular, no que diz respeito a *smart contracts* e mercados financeiros, os contratos derivados *over-the-counter* («**OTC**») parecem ser o terreno que mais convida a desenvolvimentos, sobretudo quando os respetivos ativos subjacentes sejam facilmente e fielmente representáveis em código informático (como é o caso, por exemplo, de um *swap* de taxa de juro).

O ponto central deste mercado seria a *blockchain* sobre a qual os *smart contracts* seriam inscritos e executados. Como aponta a ESMA no relatório que elaborou sobre o tema, o mais provável seria tratar-se de uma *blockchain* desenvolvida especificamente para o efeito e com acesso restrito, onde só seriam admitidos participantes específicos (*ESMA Report*. Sobre o conceito de blockchains abertas e fechadas PETERS, Gareth W./ PANAYIT, Efstathios, Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, disponível em https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2692487). O desenvolvimento e a gestão da *blockchain* estaria a cargo de uma entidade gestora, ainda que a *blockchain* seja resultado dos esforços concertados de vários atores do mercado (v.g. a R3, que está à frente de um consórcio de mais de 80 intuições financeiras: cfr. http://www.r3cev.com/about/).

O âmbito das funcionalidades que serão integradas numa primeira fase é incerto. Teoricamente, para lá das vantagens obtidas pela simples representação dos contratos em código informático (facilitando tarefas como a celebração, custódia, autenticidade e análise de contratos), seria no âmbito da compensação e da liquidação que os *smart contracts*, por via da sua integração numa *blockchains*, poderiam oferecer soluções mais inovadoras. Por essa razão, é relevante perceber em que medida as regras existentes poderiam influenciar, ou obstar, ao desenvolvimento deste mercado.

Miguel Stokes e Gabriel Freire Ramos*

* Abogados del Área de Mercantil de Uría Menéndez Proença de Carvalho (Lisboa).