RESUMO

Esta dissertação apresenta as componentes técnicas da Blockchain e dos smart contracts. Procura ainda identificar problemas jurídicos levantados por estas e oferecer soluções.

A Blockchain é uma tecnologia distribuída e descentralizada de registo eletrónico de dados. A inovação trazida pela tecnologia Blockchain é a possibilidade de cada utilizador ter uma cópia do seu registo imutável, registar informação nela e participar no seu governo. Privilegia, por regra, a transparência e elimina, teoricamente, a necessidade de intermediários ajudando a reduzir custos. A descentralização da Blockchain consiste na dissipação do controlo sobre ela. Devido à criptografia utilizada na Blockchain, esta é considerada segura. Quando à Blockchain se aliam smart contracts, as possibilidades de utilização aumentam. Os smart contracts são código que se autoexecuta e pode ser utilizado para diversas realidades como a redacção de contratos automatizados.

Todavia estas tecnologias comportam também riscos, pois podem ser utilizadas para práticas ilegais. Mais, erros e falhas no código acontecem e quando acontecerem (como já aconteceu) como reagirá a rede de utilizadores?

A Blockchain e os smart contracts levantam inúmeras questões. Como conciliar a imutabilidade da Blockchain e a necessidade de alteração desta por terem sido introduzidas informações erradas? Qual o âmbito da responsabilidade dos programadores e utilizadores destas tecnologias? Existe efetivamente descentralização se diversos utilizadores se agruparem de forma a controlarem, na prática, as regras e a informação que entra na Blockchain? Até que ponto poderá a lei regular código?

Devido à novidade destas tecnologias a regulamentação destas ainda é escassa havendo um longo caminho a percorrer. Quando se compreender melhor todas as suas potencialidades poder-se-á regulá-las melhor. Até haver uma compreensão plena destas tecnologias será melhor atender aos princípios gerais de Direito como meio de integração no sistema jurídico e identificar as jurisdições e autoridades competentes para acompanhar a evolução destas.

PALAVRAS-CHAVE: Blockchain, Código, Contratos Inteligentes, Direito

ÍNDICE

2. A Blockchain: noções fundamentais

Antes de mais nada, o que é a Blockchain?

A Blockchain é, em termos gerais, uma tecnologia distribuída e descentralizada de registo eletrónico de dados. É distribuída, ou seja, os utilizadores da Blockchain têm uma cópia actualizada da informação nela armazenada e é descentralizada, porque nenhuma entidade controla a Blockchain, sendo antes os utilizadores que, em conjunto, controlam a informação que entra nesta. Por contraste, as redes centralizadas caracterizam-se por haver uma entidade que controla e detém a informação armazenada. Trata-se, portanto, de uma base de dados digital partilhada por um conjunto de utilizadores[2], que tem como alicerce a Internet. A Blockchain consegue criar confiança entre partes que não se conhecem, sem necessidade de um intermediário, devido às suas características[3].

A informação é armazenada em blocos, ligados entre si, tornando a informação imutável. Os blocos são armazenados cronologicamente e protegidos por meio de criptografia[4]. Uma característica da Blockchain é que os dados lá

[2] Apesar da Blockchain ser descentralizada e distribuída, a tecnologia pode ser empregada em sistemas centralizados como forma de assegurar a integridade dos dados, utilizadores e/ou reduzir custos operacionais. Cf. Binance Academy, **Blockchain**, disponível em https://www.binance.vision/glossary/blockchain

[3] Estas serão desenvolvidas no capítulo 3.

[4] A criptografia é a ciência que estuda como esconder ou encriptar informação. A informação é encriptada quando se transforma determinada informação em código como meio de a proteger, escondendo-a atrás de um código que só pode ser descodificado através da utilização de uma chave de desencriptação (chave que converte o código novamente em informação).

inseridos não podem ser alterados ou apagados, conferindo a esta um elemento de segurança adicional. Esta tecnologia permite verificar e controlar muita informação de diversa natureza, desde direitos de propriedade a informação fiscal, registos médicos, e muitos outros.

Mas como funciona esta tecnologia?

A Blockchain chama-se exatamente Blockchain porque consiste, literalmente, numa cadeia de blocos. Cada bloco conterá um aglomerado de informação (data), um identificador do bloco (hash) e um hash associado ao bloco imediatamente anterior na cadeia. A única exceção é o bloco inicial que não terá o hash associado ao bloco imediatamente anterior na cadeia, por tal não existir.

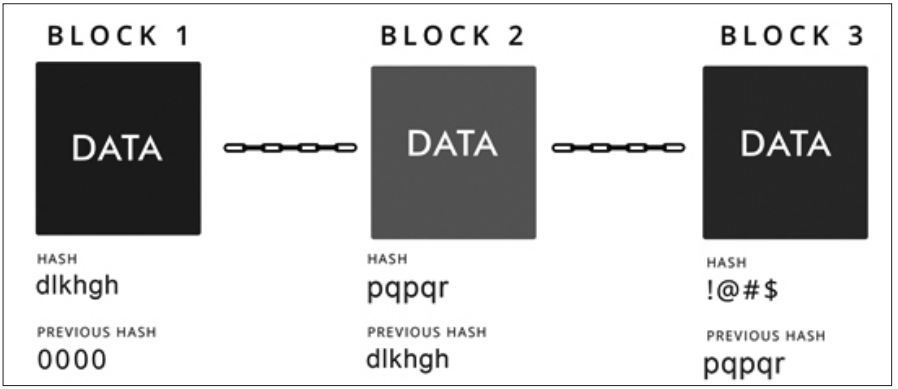

Figura 1: Imagem ilustrativa de uma Blockchain. Retirada de: https://www.blockchainexpert.uk/blog/how-does-blockchain-work

Agora, o que é um hash?

Um hash é como que um aglomerado de caracteres que identifica determinado bloco (como que a sua própria impressão digital) e este serve exatamente para identificar cada bloco e determinar a sua ordem na Blockchain conjuntamente com os selos temporais/timestamps que indicam o tempo a que o bloco foi criado. Assim o bloco 2 contém o hash que identifica o bloco 1 bem como o seu próprio hash identificador. Portanto o hash é o elemento de ligação entre os blocos.

Não obstante o que foi dito até agora aproveito para referir que, sem prejuízo destes traços caracterizadores, estamos perante uma tecnologia fluída que pode ter diversas variantes desde que se trate, na sua génese, de uma base de registo eletrónico de dados descentralizada e distribuída. Por isso, ao longo desta dissertação ir-me-ei referir à Blockchain e às diversas variantes que esta pode assumir como tecnologia Blockchain por motivos de facilidade expositiva.