**Descrição geral da criptomoeda**

A **criptomoeda** é um ativo digital concebido para funcionar como um meio de troca, utilizando a encriptação para proteger as transações e para controlar a criação de unidades adicionais de moeda. Criptomoedas são classificadas como um subconjunto de moedas digitais e também são classificadas como um subconjunto de moedas alternativas e moedas virtuais.

A Bitcoin tornou-se a primeira criptomoeda descentralizada, em 2009. Desde então, foram criadas várias criptomoedas. Estas são frequentemente chamadas de *altcoins*, como uma mistura de *alternativa de bitcoin*. A Bitcoin e os seus derivativos utilizam o controlo descentralizado em oposição aos sistemas centralizados de dinheiro eletrónico/bancos centralizados. O controlo descentralizado está relacionado com a utilização da base de dados de transações *blockchain* da bitcoin no papel de um registo (ledger) distribuído.

As criptomoedas descentralizadas são coletivamente produzidas por todo o sistema de criptomoedas , a uma taxa que é definida quando o sistema é criado e é publicamente conhecido. Em sistemas bancários e económicos centralizados, como o Sistema da Reserva Federal, os conselhos de administração ou os Governos controlam o fornecimento de moeda por unidades de impressão de moeda fiduciária, ou exigindo adições aos registos bancários digitais. No caso de criptomoeda descentralizada, as empresas ou Governos não podem produzir novas unidades e, até agora, não forneceram apoio a outras empresas, bancos ou entidades corporativas que detenham o valor do ativo avaliado. O sistema técnico subjacente à criação de criptomoedas descentralizadas, no qual estas se baseiam, foi criado por alguém (um grupo ou um indivíduo), apenas conhecido como Satoshi Nakamoto.

Em março de 2015 (data da redação originária deste texto), existiam centenas de especificações de criptomoeda; a maioria era semelhante e derivada da primeira criptomoeda descentralizada totalmente implementada, a bitcoin. Nos sistemas de criptomoeda, a segurança, a integridade e o saldo dos registos são mantidos por uma comunidade de partes mutuamente desconfiadas, conhecidas como “mineiros”. São pessoas do público em geral que utilizam os seus computadores para ajudar a validar e carimbar transações adicionando-as ao registo de acordo com um esquema de registo de data e hora específico.

A segurança dos registos de criptomoeda é baseada na suposição de que a maioria dos mineiros está honestamente a tentar manter o registo, tendo incentivo financeiro para fazê-lo.

A maioria das criptomoedas é projetada para diminuir gradualmente a produção de moeda, colocando um limite máximo na quantidade total de moeda que estará em circulação, imitando o modelo dos metais preciosos. Em comparação com as moedas comuns, detidas por instituições financeiras ou mantidas como dinheiro em caixa, as criptomoedas podem ser mais difíceis de ser apreendidas pelas autoridades policiais. Esta dificuldade é derivada do aproveitamento de tecnologias criptográficas.

Um exemplo primário deste novo desafio para a aplicação da lei vem do caso do mercado na darkweb conhecido como Silk Road, onde o stock de bitcoins do seu dono e administrador, Ross Ulbricht "foi mantido separado e... encriptado". As criptomoedas como a bitcoin são pseudónimas (e não anónimas), embora evoluções como a da Zerocoin tenham anunciado permitir o verdadeiro anonimato.

Fonte: https://en.wikipedia.org/wiki/Cryptocurrency