Criptomoedas

* O que são?

Criptomoedas não são nada mais do que meios de troca; uma forma de realizar uma transação digitalmente.

São, portanto, moedas virtuais completamente independentes do controlo dos governos, ou qualquer autoridade central, entidade, servidor, etc…

Mas se elas são completamente descentralizadas, como é que as transações são mantidas e verificadas? Porque é que elas são tão valiosas? E de onde é que vem o fornecimento dessas moedas?

Para responder a essas perguntas é preciso perceber a tecnologia inerente às criptomoedas: Blockchain.

Uma blockchain é uma espécie de livro público que regista e guarda todas as transações que alguma vez aconteceram na rede peer-to-peer dessa criptomoeda. E enquanto as transações forem uma constante e continuarem a acontecer esse registo continuará a crescer e a reconstruir-se. Essa é a razão pela qual se chama uma cadeia.

Como esse livro de registos é público para toda a gente, a sua informação vai ser continuamente distribuída e sincronizada digitalmente por todo o mundo. Ela irá partilhar sempre da mesma informação.

Quer isto dizer que, sempre que ocorre uma nova transação, ela irá ser publicamente guardada nesse livro de registos e, quando essa transação acontecer, todos os utilizadores que tiverem uma cópia desse livro serão informados da ocorrencia de uma nova transação na rede.

Às pessoas que mantêm o controle de tudo o que se passa na cadeia e que procuram verificar se as transações efetuadas são válidas e reais, chamamos “Miners”, ou em português “Mineiros”. Porquê?

Vejamos o exemplo do que se passa na Bitcoin .

Para que uma transação aconteça é necessário que se tenha uma carteira virtual na rede Bitcoin. Esta carteira incluirá duas chaves: uma privada e uma pública. Uma transação só é dada como verdadeira se for assinada pela chave privada do remetente e uma vez assinada ela está pronta para ser enviada para a cadeia de blocos com a chave pública do mesmo. Esta chave atua como um mecanismo de virificação que confirma que a mensagem do remetente foi, de facto, marcada com a sua chave privada e que esta chave está associada à sua chave pública.

Quando a transação for enviada para a rede Bitcoin, e subsequentemente anunciada a todas as pessoas que fazem a sua manutenção, estes “Mineiros” têm agora a tarefa de usar algoritmos computacionais para verificar a validade de cada transação individual.

Este processo assegura que nenhuma transação fraudolenta está a acontecer. Também é um processo extremamente complexo em que mesmo as máquinas mais poderosas podem demorar algum tempo a resolver. O primeiro nódulo a resolver essa operação recebe uma recompensa – Bitcoins – que são geradas aquando da resolução de uma das funções hash criptográfica que validam uma transação, daí a metáfora da “mineralização” das Bitcoins.

Assim que uma transação é verificada ela é acrescentada à cadeia e o processo repete-se sucessivamente.

Porém, o número de Bitcoins que um “Mineiro” recebe por recompensa não é de todo fixo, elas vão reduzindo logaritmicamente à medida que são introduzidas na cadeia, por forma a limitar o número de moedas existentes e previnir a sua inflação. Apenas 21 000 000 de Bitcoins podem estar em circulação na rede.