O Bitcoin é descentralizado?

O Bitcoin não tem uma entidade ou autoridade central. O Bitcoin não é desligável e não é censurável.

Ao utilizar a rede de comunicação global – Internet, o Bitcoin é universal e não tem limites geográficos. Os seus validadores, estando distribuídos por vários países do Mundo, tornam complexo um processo de “encerramento” ou “bloqueio” da rede, praticamente impossível.

Atualmente e segundo os dados do bitnodes.io existem 59750 nodes. Estes nodes são máquinas que correm o software bitcoin minerando as moedas, como recompensa pelas validações e confirmações de cada transação, dando suporte à rede.

Encontram-se em 134 países, distribuídos por 6434 cidades. O país com mais nodes são os Estados Unidos da América com 13358 (28.81%), a Alemanha encontra-se em segundo lugar com 5950 (cerca de 12.83%). O nosso país encontra-se em 24º lugar com 280 nodes, encontrando-se à frente de países como Dinamarca, Luxemburgo, Noruega, Israel ou Emirados Árabes Unidos.

Considerando que cada node tem na sua posse uma cópia da blockchain, isto é, uma história completa do registo de todas as transações desde o dia 12 de janeiro de 2009, compreende-se a dificuldade de tentar encerrar, desligar ou impedir o funcionamento deste sistema. Poder-se-á dizer que é uma tarefa quase impossível de concluir com sucesso!

Esta descentralização garante ao Bitcoin a segurança dos dados e, simultaneamente, a resistência à censura.

Através da distribuição da informação e dos dados, a vulnerabilidade de um ataque a um único ponto é mitigada. Neste contexto, para se alterar dados ou modificar informação no Bitcoin seria necessário fazê-lo em todos os nodes nos quais a informação se encontra armazenada. Por outro lado, para se censurar o funcionamento do sistema seria necessário intervir, simultaneamente e em coordenação em vários países, com diferentes realidades políticas, legais e diplomáticas. Banir ou ilegalizar o Bitcoin num país, não implica aplicar ou exigir a execução da mesma ordem noutro.

Poder-se-ão colocar dois cenários possíveis, mas com probabilidade reduzida: uma situação de offline total da internet ou um armagedão provocado por uma catástrofe natural ou guerra nuclear. No primeiro caso, ainda que por imposição governamental mundial, creio que todo o sistema de comunicação capitularia antes do Bitcoin, aliás somos uma sociedade, no presente momento, totalmente, dependente da internet para o bom funcionamento do nosso modo de vida moderno. No segundo caso, do pouco que, eventualmente, pudesse restar sabe-se que bastaria um node funcionar para que a rede voltasse à atividade, logo que a viabilidade funcional da internet fosse recuperada.

O Bitcoin é de facto descentralizado.