CRÓNICA DO OBEGEF
Nº 44 /2022-08-04
http://www.gestaodefraude.eu

Ricardo Passos

> > Bitcoin

A *JuicyFields* é um exemplo recente de mais um esquema de *Ponzi*. A empresa que prometia elevadas rentabilidades baseada no cultivo de canábis, desapareceu, assim como os seus responsáveis e como é óbvio desapareceu o principal: o dinheiro dos investidores.

Este caso atingiu números expressivos quer em termos de afectados, quer em termos dos montantes arrecadados. A internet é um meio que possibilita a massificação de uma mensagem e infelizmente, as pessoas que julgam que almoços grátis existem por todo o lado.

Todos os dias surgem novas oportunidades de investimento, mas a mim faz-me sempre confusão como é que as pessoas estão receptivas a investir o esforço do seu trabalho em instrumentos e soluções que muitas das vezes não compreendem. Alguns dos casos mais emblemáticos são as criptomoedas, sendo que a mais famosa é a primeira que surgiu, a Bitcoin. Não há dia em que não me falem em investir em bitcoins, que o X e o Y se "fartaram" de ganhar dinheiro com isso e porque é que em não invisto também?

Antes de investir é preciso perceber o que é a Bitcoin.

A Bitcoin assume-se como uma moeda digital descentralizada. É claro que para poder ser "moeda" tem de respeitar um conjunto de pressupostos. Tem de ser considerada como uma unidade de conta, uma reserva de valor e um meio de troca. Enquanto meio de troca tem de ser aceite por um grande grupo de entidades, as quais estão disponíveis para a aceitar. Qualquer moeda funciona com base em confiança. A Bitcoin (símbolo ₿) tem ganho alguma aceitação. Existem países que a toleram, países que a proíbem e países que a aceitam como moeda válida (El Salvador e República Centro Africana).

Pode-se dizer que a Bitcoin tem uma série de virtudes: é descentralizada, não depende de nenhuma autoridade, o livro de transações é público e distribuído e suportado numa tecnologia denominada "*blockchain*" e não existe um servidor central, mas uma rede de nós distribuída que funciona ponto a ponto. Todas as transacções são registadas em "blocos" e cada vez que há um novo "bloco" ele é adicionado à cadeia anterior. Tudo isto é salvaguardado contra transacções fraudulentas pela utilização de criptografia e pela disseminação do libro de transacções por todos os nós.

A emissão nova de moeda é feita como recompensa pelo trabalho da adição de um novo bloco de transações à cadeia. A criação de um novo bloco de transações segue um algoritmo do conhecimento público e qualquer pessoa pode tentar criar esse bloco.

Portanto tem condições para poder ser uma moeda democrática e universal.

Qual é o reverso desta moeda?

O que é possuir uma bitcoin ou parte dela? É simplesmente possuir uma grande sequência de caracteres, sequência essa que pode ser validada na rede e indica a quantidade de bitcoins que o portador possui.

Sendo anónima é um excelente meio para facilitar o branqueamento de capitais e o financiamento de actividades ilícitas. É claro que não são precisas bitcoins para isso. O velho sistema bancário, as offshores e toda uma série de instituições continuam a permitir e a contribuir para isso. Ainda agora veio a público que a fundação do príncipe Carlos de Inglaterra recebeu uma generosa doação da família Bin Laden. Falta saber a troco do quê.

O processo pelo qual se vão gerando novas bitcoins é um factor distintivo desta moeda. O processo chama-se "mineração" e é executado enquanto se gera um novo bloco para ser acrescentado à cadeia. Esse bloco contém o *hash* criptográfico (SHA-256) do bloco anterior, as novas transacções que vão ser adicionadas e um número variável (denominado "*nonce*"), de tal forma que o resultado final do cálculo do *hash* seja menor que um determinado valor pré-definido. Esse *hash* é fácil de verificar pelos nós da rede, mas encontrar um número que gere um resultado aceitável é extremamente difícil.

Em média, demora-se 10 minutos a adicionar um novo bloco à *blockchain*. Este tempo é controlado de forma que se vá mantendo mais ou menos constante independentemente da capacidade computacional empregue para gerar e descobrir o *hash*. Além disso, a cada 210.000 blocos (cerca de 4 anos decorridos), a remuneração de cada bloco é dividida por 2. Neste momento são 6,25 bitcoins por bloco. Estima-se que no ano 2140 seja atingido o número máximo de bitcoins em circulação (21 milhões) acabando a remuneração, já que nessa altura a remuneração de cada bloco passaria a ser inferior a 1 centésima milionésima de bitcoin, a unidade mínima.

Olhando para isto, é fácil de entender que a maioria das bitcoins foi gerada no início de vida da Bitcoin. Entre 2009 e 2012 foram geradas 50% do total de bitcoins que poderão existir (10,5 milhões). À data de hoje mais de 91% das bitcoins estão geradas (19 milhões). Para os próximos 120 anos existem menos de 10% do total de bitcoins por descobrir (1,9 milhões). Os primeiros que mineraram e guardaram têm uma grande quantidade de bitcoins comparados com os outros que surgiram depois e muito provavelmente alguns seriam próximos do criador da Bitcoin. Apesar de haver alguma especulação sobre o assunto ainda hoje não se sabe o nome do criador da Bitcoin. Se eu fosse um adepto da teoria da conspiração seria tentado a dizer que isto poderia ser o maior esquema de *Ponzi* alguma vez planeado, mas não tenho qualquer prova para duvidar da bondade dos intentos de quem quer que tenha inventado a Bitcoin.

Mas há algo na Bitcoin que me perturba de sobremaneira. O algoritmo de geração de novos blocos funciona em pura concorrência. O primeiro a conseguir construir um bloco válido, leva o prémio todo: as 6,25 bitcoins, mais as comissões de registar as transacções que constam no bloco (***the winner takes it all***), só que existem milhões de computadores em competição. Infelizmente todos os cálculos efectuados por quem não vence, não servem para nada! São lixo! Capacidade de cálculo utilizada em vão! Energia dissipada em aquecimento da máquina! É um desperdício que é potenciado pelo elevado valor da Bitcoin no mercado, quanto maior o valor, mais competidores tentarão a sua sorte.

A cada nova iteração, todas as máquinas têm de carregar o recém-criado bloco que passou a fazer parte da *blockchain* e começar tudo de novo: escolher novas transacções, começar com um novo número e gerar um novo *hash*, desejando que o resultado esteja dentro dos limites.

Encontrei na *wikipédia* que em média eram feitos 122.000.000.000.000.000.000.000 tentativas até conseguir gerar um bloco que cumprisse as condições (dados de Abril de 2022). São utilizados milhões de cpu's e são consumidas quantidades imensas de energia para conseguir adicionar um bloco à *blockchain*. O consumo anualizado de energia relacionada com bitcoins está estimado em 138 TWh, a mesma energia consumida durante um ano por um país como a Ucrânia, e é gerado um desperdício anual de equipamento electrónico de cerca de 34.000 toneladas, o mesmo desperdício que os Países Baixos geram.

Numa altura em que há dificuldade em obter semicondutores e em que o preço da energia tem vindo a bater recordes pelas razões que todos sabemos, havendo a necessidade de exigir a todos a redução de consumos, minerar bitcoins pode ser uma actividade perfeitamente legal, mas para mim é algo profundamente imoral. Está-se a utilizar recursos que podiam ser úteis a tanta gente a troco de uma mão cheia de nada!

A resposta à questão acima tornou-se óbvia para mim: não invisto em Bitcoin.

Nota: Esta crónica reflecte uma opinião pessoal, não do OBEGEF.