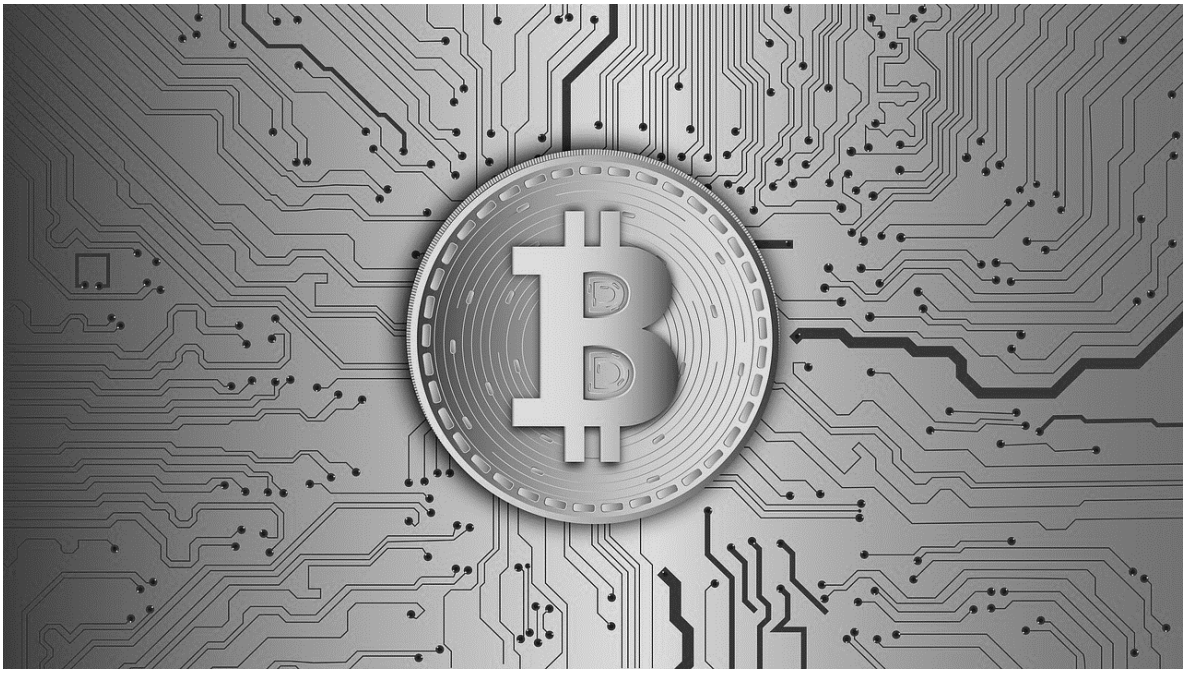
J+Legal

NEWSLETTER 2



15 perguntas que sempre quis fazer sobre *Bitcoin* (mas não teve coragem)

MANUAL J+LEGAL PARA O FASCINANTE NOVO MUNDO DAS CRIPTOMOEDAS

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

Índice

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

1. Quando nasce este novo mundo?

A *Bitcoin* é um criptoativo (já lá vamos…) que resulta de uma formulação constante de um *paper* publicado em outubro de 2008 por Satoshi Nakamoto intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*". Satoshi Nakamoto é um pseudónimo e, apesar de muitas teorias sobre o assunto, não se sabe se representa o nome de uma pessoa ou um grupo. Nesse *paper*, o(s) autor(es) descreve(m) a *blockchain,* um sistema digital *peer to peer* de pagamento e depósito sem contraparte central (sem intermediários). No início de 2009, poucos meses depois da publicação do *paper,* foi posto a circular o respetivo *softwa*re e as primeiras *Bitcoins* foram emitidas*.* O *paper* está ainda hoje disponível *online* em https://git.dhimmel.com/*Bitcoin*-whitepaper/

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

2. O que é, afinal, a Bitcoin?

A *Bitcoin* é geralmente definida como uma moeda virtual – uma divisa digital – que assenta na tecnologia *blockchain.* Não é clara, no entanto, a qualificação da *Bitcoin* – e de outras criptomoedas - como moeda ou como um mero ativo digital. Simplificando uma história longa, pode-se dizer que a moeda começou por se legitimar pelo valor intrínseco do metal em que era cunhado, passou depois a legitimar-se pela autoridade e confiança no emissor e nas suas reservas de ativos e, na medida em que os países abandonaram o chamado "padrão ouro", passou a depender da confiança na sua aceitação generalizada pelos agentes económicos num espaço geográfico – por isso se chama "moeda fiduciária" ou *fiat currency*. Ora, é certo que a *Bitcoin* ainda não é generalizadamente aceite como meio de pagamento, muito embora o seu valor seja cada vez mais reconhecido por todos os agentes. Diga-se, ainda, que outras caraterísticas (menos importantes) daquilo que qualificamos como moeda são geralmente cumpridas pela *Bitcoin* – é um ativo não disponível generalizadamente (ou seja, raro), não perecível, é divisível e transportável, assegura razoável segurança à falsificação, etc. Podemos, por tudo isso, dizer que a *Bitcoin* é um ativo digital que está no caminho de ser reconhecido como uma moeda com especiais caraterísticas. Claro que isto não é generalizável a todas as criptomoedas.

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

3. E o que é essa tal de blockchain?

A *blockchain* é a infraestrutura digital em que todo este universo repousa e, como conceito, está já muito para além do mundo das criptomoedas. Expliquemos por partes. O nosso sistema financeiro, apesar da forte digitalização que sofreu nos últimos anos, ainda assenta numa organização bastante arcaica – uma organização que depende da informação que cada banco tem (e não partilha) e de estruturas centralizadas (sejam bancos centrais, sejam câmaras de compensação, sejam outras contrapartes centrais) em que as instituições bancárias se encontram. Por extraordinário que pareça, no século XXI ainda demora três dias a creditar um cheque emitido sobre outro banco; e, quando introduzimos o elemento internacional, os prazos roçam a pornografia. A ideia central que subjaz à *blockchain* passa pela criação de uma base de dados generalizadamente acessível, sem contraparte central e com acesso descentralizado. Suponhamos que Abel quer transferir 1 *Bitcoin* para Bento – Abel tem uma *password* única (a que se chama *private key)* que lhe permite autenticar-se no sistema como o titular daquela *Bitcoin;* os computadores de Abel e Bento fazem saber todos os computadores do sistema (*"Bitcoin network"*) que pretendem fazer e receber aquela transferência*;* quando a transferência é validada, todos os participantes da rede recebem informação codificada (a transferência é registada, mas as partes são codificadas, assim se garantindo o anonimato) sobre a mesma e sobre a chave que permitirá a Bento, querendo, um dia, dispor da *Bitcoin,* atualizando e sincronizando a informação. Estamos, claro, a simplificar.

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

4. A tecnologia blockchain tem outras utilidades?

Sim. Sem dúvida. Pode-se mesmo dizer que a arquitetura descentralizada em que assenta a *blockchain* vingará sempre, independentemente do destino que venham a ter as criptomoedas, sendo hoje a base de utilizações tão diferentes como os *smart contracts* (contratos que incorporam níveis de automatismo com base em eventos determinados), uma pluralidade de funções para a *Internet of Things,* armazenamento de dados pessoais ou de outro tipo de informação (a que cada vez mais recorrem os Governos) ou ainda certificação e autenticação digital de uma pluralidade de ativos (falaremos noutra oportunidade dos *non-fungible tokens).* É também a base da chamada *Decentralized finance* (DeFi), um admirável mundo novo de organização (descentralizada) do sistema financeiro.

5. O sistema não é vulnerável?

Todos os sistemas são, de uma maneira ou de outra, vulneráveis, e a *blockchain* não é exceção – o anonimato faz com que seja muitas vezes aproximado de atividades criminosas, está sujeito a várias formas de fraude como o *phishing, Initial Coin Offerings* fraudulentas, ou falsas *wallets* com vírus/*malware*. As *Bitcoin Exchanges,* que são muito pouco, ou nada, reguladas, onde muitos guardam as suas criptomoedas, podem entrar em falência, deixando os "depositantes" totalmente desprotegidos (a falência da *exchange* japonesa Mt. Gox, em 2014, é um exemplo disto mesmo). Diga-se, em todo o caso, que o que é verdadeiramente espantoso sobre a arquitetura do *software* de *blockchain* é que este tem funcionado, desde o seu lançamento, com quase 100% de eficácia. Para se ter uma ideia do que falamos, basta dizer que o sistema suporta em cada dia mais transações do que qualquer das *money disruptor companies* como a PayPal ou a Square, sem que exista qualquer organização que o suporte ou empregados que o mantenham.

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

6. Criptomoedas = Bitcoins?

Não. De todo. A *Bitcoin* é a criptomoeda original, aquela por onde tudo começou e aquela que tem ainda hoje, de longe, a maior capitalização. Mas existem milhares de outras criptomoedas (muitas vezes chamadas de moedas digitais alternativas ou *altcoins),* num número que varia muito, mas que estará, hoje, perto da dezena de milhar. Destas, as mais importantes são a *Ethereum*, a *Bitcoin Cash*, a *Litecoin*, a *Ripple*, a *Stellar* e a *Cardano*. Cada uma destas *altcoins* assenta na sua própria plataforma de *blockchain* e procura introduzir diferenciações face à *Bitcoin* (escalabilidade, segurança, velocidade de transação, elementos de *stable coin,* etc). É de esperar que, nos próximos anos, e independentemente do sucesso ou fracasso geral das criptomoedas, vários destes projetos alternativos venham a soçobrar, pelo que se pode afirmar que quanto mais recente e exótica é a *altcoin* maior é o risco de perda total do investimento (e, claro, maior é a sua valorização potencial).

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

7. O que é a mineração de criptomoedas (crypto mining)?

A mineração das *Bitcoin*s (ou de outras criptomoedas) é parte essencial do funcionamento do sistema. É apresentada como uma atividade informática em que sistemas de *hardware* funcionam de forma a "descobrir" *Bitcoin*s, que são libertadas pelo algoritmo. Esta ideia quer aproximar a atividade à mineração de metais preciosos. Mas não é bem assim. Os mineradores, na verdade, funcionam como auditores do sistema e verificam, em rede descentralizada, a correção das transações e a sua reconciliação. Cada vez que o minerador verifica 1 *megabyte* de transações, é elegível para ser remunerado em *Bitcoin*s (ser elegível, significa que pode ser remunerado, ou não, dependendo da sua sorte e da capacidade de resolver o algoritmo). Estamos, de novo, a simplificar o sistema. Diga-se ainda, que estas remunerações são a única forma primária de introduzir *Bitcoin*s no sistema.

8. Compensa minerar criptomoedas?

A mineração de criptomoedas consome, quer na computação, quer na refrigeração, muita energia. Há, aliás, controvérsia sobre os custos ambientais desta atividade. Por isso, a sua rentabilidade em grande escala depende sobretudo de dois fatores variáveis – o valor da criptomoeda e o custo da energia – e de um de *capex* – o custo do *hardware,* sobretudo das placas gráficas (que, graças à *Bitcoin,* estão hoje praticamente esgotadas no mercado). Sem surpresa, os países com mais mineração têm todos eles custos baixos de energia – China, EUA, Rússia, Cazaquistão, Malásia e Irão. Claro que se faz muita mineração "doméstica", de pequena escala, em países como Portugal, o que pode proporcionar algum lucro (sem grande margem). Existem ainda várias formas de organização em *pool* para atividades de mineração (sendo que muitas delas são fraudulentas).

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

9. É legal investir em criptomoedas?

A resposta a esta pergunta depende do país a que nos referimos. A maior parte dos países – e entre eles Portugal – não tem regulamentação própria para as criptomoedas. No entanto, nada permite entender que o facto de ser um ativo não regulado faz com que não seja legal investir em criptomoedas. A resposta é assim afirmativa. Um segundo grupo de países – por exemplo, Alemanha, EUA, Suíça ou Luxemburgo – tem vindo a regular o tema como forma, normalmente, de o tratar fiscalmente ou de lhe dar estabilidade e atrair investimentos. Também nestes casos a resposta é afirmativa. Temos por fim um grupo de países que tem regulado o tema no sentido da sua proibição – nuns casos proibição total (Egito, Marrocos, etc) e noutros casos criando restrições à circulação de fundos bancários de e para criptomoedas (China, Canadá, etc). Para uma economia aberta e periférica como a nossa, com vocação para a economia digital, dir-se-ia que o bom caminho seria a regulamentação favorável desta nova realidade, como forma de atrair investimento, centros de competências e criação de trabalho qualificado.

10. A criptomoeda vai substituir o ouro como reserva de valor?

Ninguém pode dar uma resposta segura a esta pergunta. Os grandes defensores da *Bitcoin* acreditam que sim e salientam as suas vantagens comparativas – grande liquidez, profundidade do mercado, finitude (em alguns casos), não perecimento, transportabilidade, etc. A verdade, porém, é que o ouro, como reserva de valor, tem uma história de muitos séculos que o transformam num "porto seguro" para investidores. Nos dias que correm, podemos olhar para os dois ativos como parte de estratégias de diversificação e de *hedging* para riscos como a desvalorização (e cada vez mais bancos aceitam esta aproximação).

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

11. Como posso comprar criptomoeda?

As criptomoedas não funcionam em mercados organizados e regulamentados. Isto significa que os mercados em que são transacionadas – as *crypto exchanges* – funcionam de forma independente e não centralizada. Assim, na prática, os preços podem variar, no mesmo momento, de *exchange* para *exchange* (claro que o facto de já haver muitos investidores a fazer arbitragem diminui sempre esse *delta*) e os custos de transação também variam enormemente. Apesar da ainda limitada regulamentação que existe, é também aconselhado escolher uma *exchange* que funcione num ambiente com alguma regulamentação, como o norte-americano, porque isso dá alguma segurança aos investidores. À data, as maiores exchanges são a *Binance*, a *Coinbase*, a *Kraken*, a *Huobi* e a *Bitfinex*. Alternativas à aquisição de criptomoeda em mercado passam pela aquisição de derivados sobre criptomoeda (muitas vezes com alavancagem), a aquisição de criptomoeda em oferta inicial ou ainda a aquisição de unidades de participação em fundos de investimento (alternativos).

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

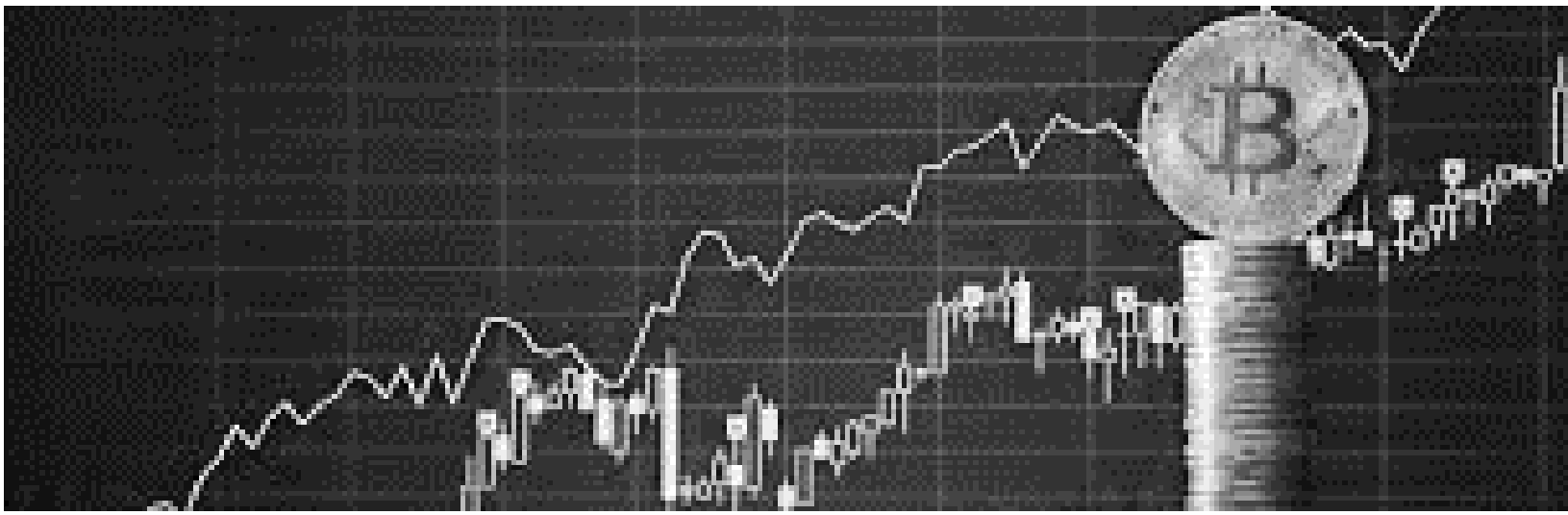
12. Como posso guardar criptomoeda?

Na verdade, existem várias formas de o fazer. Quem compra criptomoedas recebe uma *private key* e é o armazenamento dessa *private key* que permite legitimar perante o sistema a titularidade da moeda. Para isso, a *private key* deve ser guardada numa *wallet.* Existem no mercado dois tipos de *wallet* – as *hot wallets,* que funcionam associadas a qualquer tecnologia com ligação à internet como computadores ou telefones e as *cold wallets,* que são como que uma *pen* sem qualquer ligação à internet e que podem ser conectadas ao sistema se e quando o proprietário o pretenda através de um *software* específico. Apesar de as *hot wallets* serem muito mais práticas, sobretudo para quem faça habitualmente *trading* de criptomoeda, é geralmente reconhecido que têm maiores riscos. Escusado será dizer que, quer num caso, quer no outro, o acesso à *wallet* depende de uma *password* que, se perdida, faz com os ativos fiquem inacessíveis para sempre. Outra forma de guardar criptomoeda é fazê-lo na carteira própria que quase todas as *crypto exchanges* proporcionam. Aqui os riscos são de dupla natureza – por um lado, o investidor está sujeito aos riscos de *hacking* que qualquer plataforma digital tem; mas, por outro, suporta o risco de falência da *exchange* (já que ele é apenas credor dos ativos e não proprietário, de onde resulta que está sujeito aos riscos de insolvência, sem a garantia do Estado, ou de fundos de garantia, para os depósitos bancários). Por fim, quando os investidores adquirem – sobretudo em plataformas *fintech* – derivados sobre criptomoedas, a segurança do investimento dependerá dos termos do derivado e da solidez do custodiante.

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

13. O investimento em criptomoedas tem mais riscos que outros investimentos?

A resposta a esta pergunta não é fácil, mas, de um modo geral, será afirmativa. O facto de este ser um mundo novo, com produtos novos e atores novos (alguns dos quais desaparecerão daqui a algum tempo, como resultado do próprio funcionamento das regras de mercado) introduz fatores de risco adicionais. Somado a isto, como a CMVM salientou em documento preparado há algum tempo, somam-se riscos de liquidez, agravados no caso das *altcoins,* risco de perda total dos montantes investidos, risco de insuficiência de informação, risco de fraude, uma volatilidade que por vezes é levadíssima e, não menos importante, risco de alteração do quadro legislativo. A não regulação, que para alguns é uma vantagem, é para outros uma desvantagem e propicia valorizações e desvalorizações abruptas, negociação *non-stop* (um dos maiores momentos de valorização dos últimos meses foi no dia de Natal e durante a quadra festiva). Para uns isto é inspirador; para outros é um retrato do inferno. Ainda assim há que reconhecer que, num momento de grande imponderabilidade macro/económica, poderá ser um ativo de proteção face à (desejada?) inflação, o que poderá até estar a influenciar negativamente a evolução da cotação do ouro.



Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

14. As mais-valias com a transação de criptomoeda pagam impostos?

Depende. No caso das pessoas coletivas, como todo o acréscimo anual de património é tributável (rendimento acréscimo), a resposta é afirmativa. Passível de discussão é apenas o momento do reconhecimento do rédito (na realização ou por *mark to market*). Para as pessoas singulares, o exercício de especulação sobre criptomoedas, como atividade económica, será tributado como qualquer atividade de *trading* (na categoria B de IRS, portanto). Já os ganhos ocasionais decorrentes da detenção de moeda não o serão, como não o são os ganhos cambiais noutras divisas. No entanto, ganhos sobre derivados poderão cair no âmbito de incidência da Categoria E do IRS. Do lado da tributação indireta, são operações fora do campo do IVA, precisamente pela sua qualidade de "moeda". Para efeitos de sucessões e doações parece ser de entender que são ativos localizados fora do território nacional e, por isso, fora do âmbito de incidência do imposto do selo.

15. E pagarão impostos no futuro?

Como a morte e os impostos são certos e, dada a crise económica que se antevê, os Estados terão de alargar (brutalmente) as bases tributáveis, é muito plausível que o venham a ser. Ou por alargamento da tributação em IRS aos meros ganhos cambiais ocasionais, ou ainda por uma verba específica em imposto do selo sobre estas operações financeiras, ou por fim no quadro de um eventual (e indesejável) imposto sobre o património, geral ou financeiro. Certo é já a sua regulamentação acrescida no quadro europeu, como o demonstram as DAC 7 e 8. O que reforça a ideia do bom caminho para Portugal de criar uma regulamentação favorável para este novo ecossistema e assim captar investimento e criar centros de competências e empregos qualificados.

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

Contactos

Jorge Brito Pereira
Sócio da Área de Banking & Capital Markets
jbp@jlegal.pt

Jaime Carvalho Esteves
Sócio da Área de Tax
jce@jlegal.pt

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt

J+Legal

Edifício Amoreiras Square
Rua Joshua Benoliel 1, 6º C, 1250-273 Lisboa - Portugal E.: geral@jlegal.pt T.: (+351) 218 770 000 jlegal.pt