

# CRIPTOATIVOS

---

SÉRIE ALERTAS



# CRIPTOATIVOS

Os criptoativos são ativos virtuais, protegidos por criptografia, presentes exclusivamente em registros digitais, cujas operações são executadas e armazenadas em uma rede de computadores.

Esses ativos surgiram com a intenção de permitir que indivíduos ou empresas efetuem pagamentos ou transferências financeiras eletrônicas diretamente a outros indivíduos ou empresas, sem a necessidade da intermediação de uma instituição financeira. Tal propósito serviria - inclusive - para pagamentos ou transferências internacionais.

Atualmente existem centenas de criptoativos, dentre os quais o pioneiro e mais conhecido é o Bitcoin. Cada um deles funciona baseado em um conjunto de regras próprias, definidas pelos seus criadores e desenvolvedores.

O funcionamento dos criptoativos se baseia em uma **tecnologia de registro descentralizado**<sup>1</sup>, um tipo de contabilidade ou livro-razão distribuído em uma rede **ponto a ponto**<sup>2</sup> de computadores espalhados ao redor do mundo. Toda transação realizada é divulgada para a rede, e somente será aceita após um complexo sistema de validação e de uma espécie de consenso da maioria dos participantes da rede. Com isso, as operações são praticamente irreversíveis, por exemplo: se um proprietário tentar reutilizar ativos já negociados (o chamado “gasto duplo”), a rede de computadores rejeitaria a transação, característica essa que eliminaria a necessidade de um intermediário.



A tecnologia mais conhecida por trás do funcionamento dos criptoativos ficou conhecida como *blockchain*. Isso porque nela as transações publicadas na rede são agrupadas e registradas em blocos, de maneira que cada bloco aceito na rede se conecta ao imediatamente anterior, e assim por diante, formando uma sequência ou cadeia de blocos (*blockchain*).

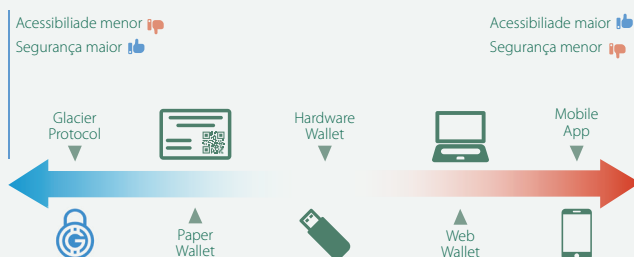
A propriedade desses ativos virtuais não é verificada pela comprovação da identidade de seu detentor, mas sim por uma senha secreta que, por meio de técnicas de criptografia, permite que as transações sejam realizadas de forma quase anônimas, sem que as partes tenham que revelar quaisquer informações que não desejem.

<sup>1</sup> DLT, ou *Distributed Ledger Technology*.

<sup>2</sup> *Peer-to-Peer*, ou P2P.

Assim, quem possuir a senha se torna o proprietário dos criptoativos. Esses ativos podem ser negociados através de plataformas eletrônicas (*Exchanges*) ou bilateralmente, em negócios sem intermediação.

Para operar com um criptoativo é preciso possuir pelo menos uma conta virtual, chamada de “carteira virtual” (*wallet*)<sup>3</sup>, com uma chave pública, para publicar as transações na rede, e a chave privada secreta, necessária para ter acesso à carteira e poder operar com ela. Existem diferentes tipos de carteiras, definidas de acordo com a maneira como são armazenadas, ou custodiadas. Na prática, como a imagem a seguir demonstra, existem diferentes soluções para isso. Note que as soluções *cold wallet*, embora mais seguras, são menos acessíveis, o contrário das propostas *hot wallet*.



Note que os criptoativos, especialmente quando criados para realização de pagamentos ou transferências financeiras, como é o caso do Bitcoin, não são emitidos, controlados, garantidos ou regulados por qualquer autoridade monetária, o que significa dizer que eles compõem um universo totalmente separado das moedas oficiais, como o dólar ou o real. Desse modo, a aceitação desses ativos virtuais como meio de pagamento não é mandatária. Além disso, a alta volatilidade dos preços dos criptoativos indica que eles não são adequados para assumir duas das três funções de uma moeda oficial: unidade de conta e reserva de valor.

Os criptoativos também não se confundem com as chamadas moedas eletrônicas, previstas na legislação brasileira, que nada mais são do que recursos em reais mantidos em meio eletrônico em uma dada instituição financeira, e que podem ser utilizados como meio de pagamento, assim como as notas físicas de real.

**Os criptoativos não residem em registros digitais de nenhuma instituição financeira.**

<sup>3</sup> Uma wallet pode ser entendida como um programa para gerenciar criptoativos.



## Oferta Inicial de Ativos Virtuais (*Initial Coin Offering* – ICO)

---

Com o passar do tempo, vislumbrou-se que as tecnologias que viabilizavam o funcionamento dos primeiros criptoativos, como o Bitcoin, poderiam ser usadas para outras finalidades. A rede distribuída de computadores deixaria de fazer apenas o registro e a validação de transações, e poderia também rodar programas, registrar contratos e executá-los de forma autônoma, sem intervenção de intermediários.

A possibilidade de traduzir um contrato em código-fonte e confiar sua execução a uma rede distribuída de computadores trouxe inúmeras possibilidades de aplicação. A primeira grande manifestação do potencial desse novo uso da tecnologia foi o fenômeno dos ICOs (*Initial Coin Offerings*), ou oferta inicial de ativos virtuais.

Empresas ou projetos em estágio inicial de crescimento encontraram no ICO uma ferramenta para captar recursos financeiros junto ao público. Em troca, emitem ativos virtuais em favor dos investidores. As denominações mais comuns desses ativos virtuais emitidos são criptomonedas ou *tokens*.

Os *tokens*, que conferem direitos diversos aos seus detentores, podem ser divididos em pelo menos duas categorias, a depender do tipo de direito concedido: *tokens* que concedem acesso a um serviço, plataforma ou projeto da empresa, nos moldes de uma licença de uso ou de créditos para consumir um bem ou serviço; e *tokens* que conferem aos investidores direitos de participação em resultados do empreendimento, ou remuneração pré-fixada sobre o capital investido, ou ainda voto em assembleias que determinam o direcionamento dos negócios do emissor.

O que determina se uma operação de ICO estará ou não sujeita à regulamentação do mercado de valores mobiliários é a natureza dos ativos virtuais emitidos na operação. Se os direitos caracterizarem o ativo como valor mobiliário, a operação, os emissores e demais agentes envolvidos estarão obrigados a cumprir a legislação e a regulamentação da CVM.

As ofertas de ativos virtuais que se enquadrem na definição de valor mobiliário e estejam em desconformidade com a regulamentação serão tidas como irregulares e, como tais, estarão sujeitas às sanções e penalidades aplicáveis.

**A CVM alerta que, até a presente data, não foi registrada nem dispensada de registro nenhuma oferta de *tokens* cujos direitos os caracterizem como valores mobiliários.**



## Muito cuidado!

---

As características inerentes ao mercado de criptoativos deixam clara a existência de potenciais riscos aos usuários e investidores. Alertamos abaixo para alguns desses riscos, sem a pretensão de esgotar o assunto.

### Risco de fraudes

O mercado de criptoativos tem sido objeto frequente de fraudes cometidas por criminosos que são atraídos pelo perfil transfronteiriço das operações, pelo anonimato e por outras particularidades desse mercado. Entre os crimes mais comuns estão o estelionato, pirâmides financeiras e esquemas “Ponzi”, que se caracterizam, em geral, pela divulgação de informações falsas sobre projetos ou serviços, oferta de ganhos exagerados ou garantidos, ou ainda um sistema de remuneração alimentado pela entrada de novos participantes.

Esse mercado também tem sofrido com crimes de manipulação, realizados por meio de esquemas organizados de divulgação de notícias falsas e estratégias de marketing, com o único intuito de inflar os preços para vender os ativos (chamados esquemas de “*pump&dump*”).

### Risco de liquidez e alta volatilidade dos ativos virtuais


Liquidez em finanças pode ser entendida como a facilidade com que determinado ativo pode ser convertido em moeda (vendido) a um preço justo. No que se refere aos criptoativos, portanto, risco de liquidez é o risco de não encontrar comprador para certa quantidade do criptoativo ao preço cotado em mercado. Tal risco pode limitar a possibilidade de se converter o ativo em moeda fiduciária, ou então acarretar perdas potenciais caso se decida vendê-lo a qualquer valor.

Além disso, os preços de negociação desses criptoativos têm apresentado alta volatilidade, o que pode provocar perda parcial ou total do valor nelas aplicado.

### Riscos específicos da não regulamentação ou do caráter transfronteiriço das operações

Quando não regulamentados, mercados apresentam riscos operacionais relacionados a ambientes de negociação, ativos virtuais e sistemas não monitorados pelos reguladores. Nesses casos, as informações divulgadas e o material publicitário da oferta não necessariamente observam a regulamentação da CVM, e os prestadores de serviços atuam sem observância à legislação aplicável ao mercado de capitais.

No que se refere à custódia desses ativos virtuais, os investidores podem ficar expostos a riscos relacionados ao armazenamento de senhas de criptografias e de custódia. Há muitos casos de perda de bitcoins e outros criptoativos em razão do desaparecimento de senhas, ou devido a ataques a carteiras pouco seguras, conforme o tipo de solução adotada para a custódia.



Vale ressaltar, ainda, que a inexistência de processos formais de adequação do perfil do investidor ao risco do empreendimento (*suitability*) aumenta a possibilidade de expor os investidores a riscos por vezes maiores do que estariam dispostos ou do que seriam capazes de assumir.

Ademais, os diversos participantes envolvidos na emissão, custódia e negociação dos ativos virtuais, como as plataformas de negociação, os emissores e outros agentes, podem não estar localizados no Brasil, de maneira que a resolução de qualquer conflito pode estar fora do mandato das autoridades brasileiras, o que sinaliza a existência de desafios jurídicos e operacionais em casos de litígio com outros participantes do mercado.

### Riscos cibernéticos

Os ativos virtuais apresentam forte dependência de tecnologias ainda não consolidadas, o que os expõe a possíveis falhas operacionais e ameaças cibernéticas associadas à gestão e custódia dos ativos, como ataques à infraestrutura ou aos sistemas, e comprometimento de credenciais de acesso, que podem implicar a indisponibilidade temporária ou mesmo a perda total dos valores investidos.

Para evitar fraudes e reduzir os riscos associados a essas operações, **fique atento:**

- Quando se deparar com um anúncio de ICO, verifique no site da CVM se o ofertante é emissor registrado na autarquia ou se a oferta foi registrada ou dispensada de registro;
- Avalie atentamente as características da operação para evitar sinais de irregularidade, como rentabilidade alta ou garantida; inexistência de taxas; pressão para participar das transações imediatamente; ofertantes ou ofertas não registradas na CVM; falta de requisitos mínimos para participar, entre outros; e
- Em caso de dúvidas, denúncias ou reclamações, acesse os canais de atendimento ao investidor da CVM.

## Fale com a CVM

Para consultas, reclamações e sugestões, utilize os canais abaixo:

### Internet

Serviço de Atendimento ao Cidadão (SAC)  
[www.cvm.gov.br](http://www.cvm.gov.br) > Atendimento

### Telefone

Consulte o número em [www.cvm.gov.br](http://www.cvm.gov.br)>Atendimento

### Carta / Pessoalmente

Superintendência de Proteção e Orientação aos Investidores:

- RJ: Rua Sete de Setembro, 111 - 5º andar - CEP 20050-901
- SP: Rua Cincinato Braga, 340 - 2º andar - CEP 01333-010



[www.cvm.gov.br](http://www.cvm.gov.br)



[www.investidor.gov.br](http://www.investidor.gov.br)



[cursos.cvm.gov.br](http://cursos.cvm.gov.br)



[pensologoinvesto.cvm.gov.br](http://pensologoinvesto.cvm.gov.br)



CVMEducacional



CVMEducacional



CVMEducacional



CVMEducacional



company/CVM

# CRIPTOATIVOS

---

S É R I E   A L E R T A S



MAIO 2018