Inter Research: CriptoWorld Ed.5.21

Geração X, Y, Z? As diferentes gerações das criptomoedas

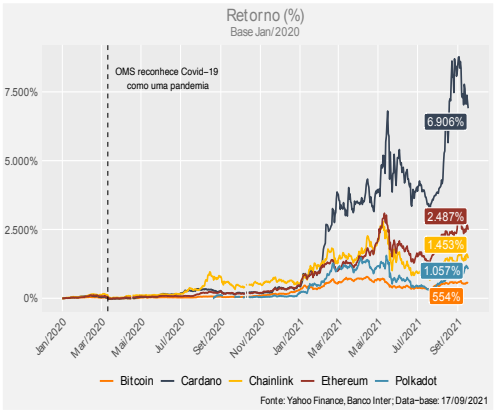
Assim como somos classificados em gerações, cada uma com suas características mais marcantes, as criptomoedas também apresentam diferentes características que as colocam dentro de uma geração específica. Já comentamos sobre essas diferenças anteriormente, mas nesta edição, decidimos ir mais a fundo para te explicar quais os diferenciais de cada uma destas gerações e o que esperar para o futuro.

Boa leitura!

Ativo	Δ% 1Mês	Δ% Ano	Δ% 12m
Vitreo Cripto Metals	1,9%	13%	20%
Vitreo Criptomoedas	4,1%	102%	212%
Hashdex 20 N. Crypto	1,0%	23%	45%
Hashdex 40 N. Crypto	1,7%	44%	102%
HASH11	5,9%	-13%	-13%
QBTC11	3,9%	51%	51%

(em 16/09/21)

Desempenho dos ativos



Fonte: Bloomberg

1 ª Geração das Criptomoedas

O Bitcoin tem se mostrado bastante resiliente nos últimos 12 anos desde seu surgimento. Apesar de sua alta volatilidade, podemos dizer que essa criptomoeda cumpriu sua função principal. Qualquer pessoa com acesso à internet pode verificar todas as transações que já ocorreram dentro da sua blockchain, sem discriminação de informação, com todos os detalhes da tecnologia disponíveis e sem necessidade de pedir permissão para seu uso. É como se uma empresa tornasse público todos seus bancos de dados e liberasse o acesso a todos seus sistemas, e, mesmo assim, nenhuma pessoa com má intenção ou hacker conseguisse tirar proveito dessa situação.

Contudo, o alto nível de segurança da tecnologia por trás do Bitcoin o torna extremamente resistente a mudanças, inclusive as que possivelmente seriam positivas. Apesar de vários discordarem dessa perspectiva, tal característica não é necessariamente ruim, e talvez seja uma condição necessária para seu sucesso.

Recentemente, uma sugestão de mudança aparentemente inofensiva e positiva, como a de aumentar o espaço disponível por bloco minerado na Blockchain, foi motivo de bastante discussão e conflito na comunidade cripto. Quem apoiava a mudança defendia que mais espaço para armazenamento significaria que mais transações poderiam ser registradas por bloco, o que aumentaria a velocidade e tornaria menos custoso o ato de comprar e vender bitcoins. Por outro lado, o grupo contrário, que hoje seriam identificados como Bitcoin Maximalists usavam o famoso argumento de que “não se mexe em time que está ganhando” e, em última análise, o que fez com que o Bitcoin chegasse aonde chegou era justamente sua imutabilidade e previsibilidade. Mudanças, mesmo que aparentemente inofensivas, abrem espaço para mais mudanças potencialmente prejudiciais.

Gabriela Cortez Joubert, CNPI
gabriela.joubert@bancointer.com.br

Fernando Urbano
fernando.rocha@bancointer.com.br

Vitor Carvalho
vitor.carvalho@bancointer.com.br

Os desenvolvedores do Bitcoin foram pioneiros ao criar um sistema de pagamentos descentralizado, isto é, que não dependesse da confiança em terceiros, e sim de poder computacional gerado pela rede como um todo. Tal façanha só foi possível por meio do uso de uma estrutura de incentivos que permitiu o alinhamento dos interesses entre os mineradores e os usuários e por meio de uma estrutura extremamente segura, porém mais engessada.

Já falamos aqui sobre esse *tradeoff* entre segurança e funcionalidade. O Bitcoin é uma das criptomoedas mais seguras do mundo. Mas, o que acontece quando se abre o leque para novas funcionalidades, mesmo que em certo detrimento da segurança?

2 ª Geração das Criptomoedas

Outro *insight* de sucesso que inaugurou a segunda geração das criptomoedas, foi o entendimento de que o uso da tecnologia Blockchain não precisaria estar limitado apenas ao ato de realizar transações. Seria possível realizar estas transações, mas sujeita-las a diferentes condições previamente estabelecidas e mutualmente aceitas. Um exemplo seria permitir que você envie recursos para seu amigo se, e apenas se, hoje for quarta feira. Apesar de extremamente simplista, este exemplo demonstra bem qual era objetivo dos idealizadores da segunda plataforma mais famosa, a Ethereum (falamos dela na última edição sobre NFTs aqui).

O lançamento da Ethereum permitiu a funcionalidade de uma transação sujeita a condições programada em uma blockchain, ou seja, os Smart Contract, ou contrato inteligente.

Uso dos Smart Contracts

Para quem está familiarizado com o mercado financeiro, sabe o que são os derivativos como opções de compra e venda. O mercado de derivativo é enorme e envolve muitos riscos. Além dos riscos relacionados à variação dos preços, há o risco de contraparte e o risco do próprio intermediário que armazena informações do contrato. Por ter uma estrutura relativamente simples e riscos consideráveis, esses são os tipos de contratos perfeitos para lançar em uma blockchain.

Essa ideia é apenas uma das inúmeras aplicações do universo que hoje chamamos de *Descentralized Finance ou DeFi*. Atualmente, há mais que 100 bilhões de dólares investidos neste setor.

O Problema do Oráculo

Porém, para que o *DeFi* emergisse, era necessário resolver um importante problema. Informações *on chain* são aquelas que são geradas pela própria blockchain e as únicas que o protocolo pode interpretar por conta própria. Entretanto, esses dados como data, quantidade, bits, chaves, operações matemáticas e de lógica, não são suficientes para arquitetar a maior parte dos contratos que hoje fazem parte do nosso cotidiano. Logo, como ter acesso a informações que não são fornecidas *on chain*? Esse questionamento é conhecido como "Problema do Oráculo"

Para fazermos um contrato futuro sobre o café, a Blockchain onde está armazenado o contrato precisaria ter acesso ao preço dessa commodity, já que essa informação pode alterar as obrigações das partes envolvidas. Logo, alguém de confiança precisaria providenciar esse tipo de dado cuja origem é *off chain* (fora da blockchain).

A comunidade cripto entende que o diferencial das criptomoedas é gerar uma estrutura de obrigações em que não haja a necessidade de se confiar em absolutamente ninguém a não ser na própria tecnologia. Portanto, a qualidade dos dados providenciados por um bom oráculo deve se aproximar ao máximo do nível de confiabilidade exigida pelos usuários de diferentes blockchains.

A Chainlink (LINK), por exemplo, é uma plataforma de blockchain que busca solucionar o problema do oráculo. Hoje, somente essa rede proporciona mais de 50% de todos os dados off chain usados pelas diferentes aplicações DeFi. Para providenciar dados de alta qualidade, a Chainlink usa inúmeras fontes para obter uma mesma informação, além disso, faz uso de toda uma estrutura de incentivos semelhante àquela usada por criptomoedas como o Bitcoin. Quem deseja participar da blockchain como validador e, portanto, ser remunerado por isso, deve se submeter ao processo de se tornar *stakeholder* e alocar seu próprio patrimônio na rede. Ou seja, validadores

precisam ter "*skin in the game*". Esse é um sistema conhecido como *Proof of Stake*.

Resumindo, após uma única informação ser gerada pelo consenso de diversas fontes, antes de ser passada de fato para uma aplicação on chain, tal informação ainda é processada por toda uma equipe de milhares de validadores stakeholders que têm muito a perder, caso estejam fornecendo dados falsificáveis. E esse é o nível de segurança e descentralização aceitável pela comunidade cripto.

Com isso, passamos para a terceira geração das criptomoedas.

3 ª Geração das Criptomoedas

Por fim, a Cardano pode ser considerada como pioneira da terceira geração das criptomoedas. Cardano é mais maleável e permite mudanças no protocolo de forma mais simples e menos burocrática. É importante ressaltar, todavia, que a Cardano ainda faz uso da blockchain e, assim, faz jus a diversos requisitos de segurança, como descentralização, imutabilidade e respeito a anonimidade.

Quando dizemos que há um *tradeoff* entre segurança e usabilidade nas blockchains, é importante ressaltar que sempre haverá requisitos mínimos a serem cumpridos para pelo menos fazer uso dessa tecnologia. Para exemplificar o que isso significa, basta pensar no protocolo das criptomoedas da mesma forma que pensamos na constituição de um país. Quase todas as democracias possuem constituições que estabelecem limites invioláveis independente do político que esteja no poder. Todavia, dentro deste expecto legal, é possível sugerir mudanças que, geralmente, vão de encontro ao interesse da maior parte da população, já que teoricamente foi a maioria que elegeu o governo que sugeriu a proposta em primeiro lugar. Esse processo é feito por meio de emendas constitucionais, no caso brasileiro, conhecidas como PECs.

Todas as blockchains possuem um bloco gênese que estabelece um protocolo ou uma "constituição" com limites invioláveis, o que varia é o grau de burocracia e consenso necessário para que certas variações sejam implementadas. No Ethereum, por exemplo, os EIP's (Ethereum Improvement Proposals) sistematizam o processo de solicitar upgrades, da mesma forma que as PECs são utilizadas em nosso sistema constitucional. Assim, o Ethereum apresenta ordens de grandeza mais "aberto" que bitcoin. A ambição dos desenvolvedores da Cardano (ADA), por outro lado, está em outro nível.

Para começar, **a equipe por trás da Cardano deseja criar uma "internet de blockchains".** A internet faz parte de nosso cotidiano na atualidade, é simples entendermos que não é possível determinar o que seria o "melhor site", principalmente quando tentamos comparar os que foram criados para cumprir diferentes propósitos. Por exemplo, o Google cumpre bem seu papel de ser uma ferramenta de pesquisa, o Instagram é uma excelente rede social para publicação de fotos e vídeos relativamente curtos, o site da Amazon e Mercado Livre foram disruptivos na ideia de um marketplace para quem deseja realizar compras online, e por aí vai. Todos esses domínios são controlados por diferentes empresas que seriam capazes, caso tivessem interesse, de incorporar todas essas funcionalidades em uma única plataforma, já que a base da tecnologia é a mesma.

Segundo os idealizadores por traz do projeto da Cardano, este fenômeno também ocorre no mundo das criptos. Por exemplo, podemos dizer que o Bitcoin é muito eficiente em permitir que as pessoas façam transações não complexas entre si, além de ser considerado um ativo digital seguro, como o ouro é para o mercado financeiro tradicional. Ethereum, por outro lado, permite programar e fazer uso de contratos inteligentes de forma extremamente acessível. Chainlink é eficiente em fornecer dados confiáveis da vida real off chain para aplicações de diferentes protocolos. A blockchain da Binance é responsável pelo funcionamento de toda uma Exchange onde é possível comprar diversas outras criptomoedas e produtos financeiros e, por isso, foi arquitetada de forma a ser capaz de suportar milhares de transações por segundo.

Assim, um grande obstáculo para a ascensão das criptomoedas, é a falta de um mecanismo que sistematize a comunicação entre as diferentes blockchains, do mesmo modo que o HTTPs foi revolucionário em seu tempo ao permitir que a navegação na internet fosse fluída e intuitiva, do jeito que estamos acostumados hoje em dia. Essa é a ambição da terceira geração das criptomoedas. Há pessoas extremamen-

te dedicadas, como as que estão por trás de projetos como Cardano e Polkadot, trabalhando nisso no exato momento em que você lê esse texto.

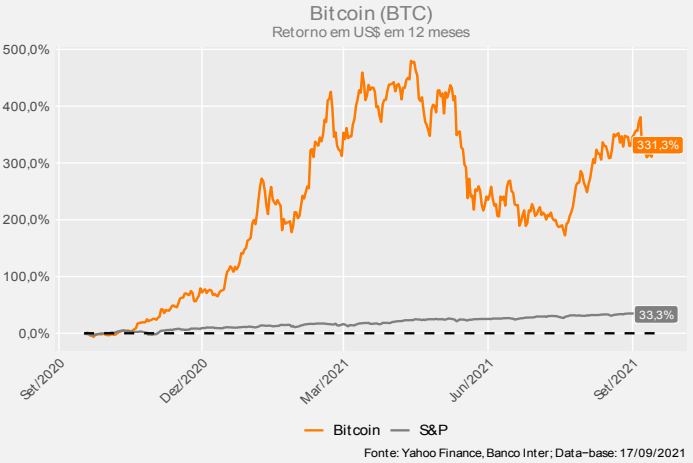
O que veremos para as próximas gerações? Ouse imaginar!

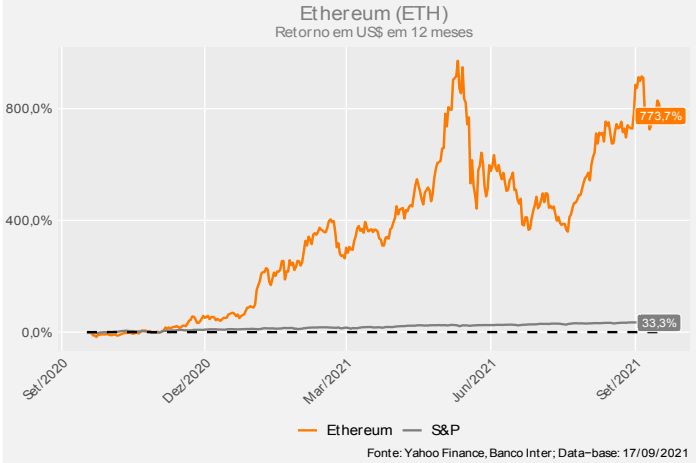
Vale lembrar sempre que no Brasil a CVM não considera as criptomoedas valores mobiliários e não existem corretoras autorizadas pelo Sistema Financeiro Nacional a transacioná-las. No entanto, o investimento na classe é possível por meio de fundos de investimento com estratégias de investimento no exterior.

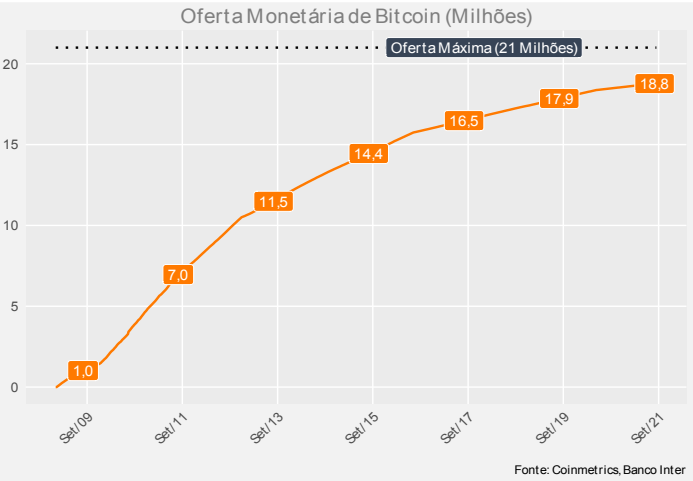
No Inter, você pode investir em criptoativos através dos seguintes fundos e ETFs:

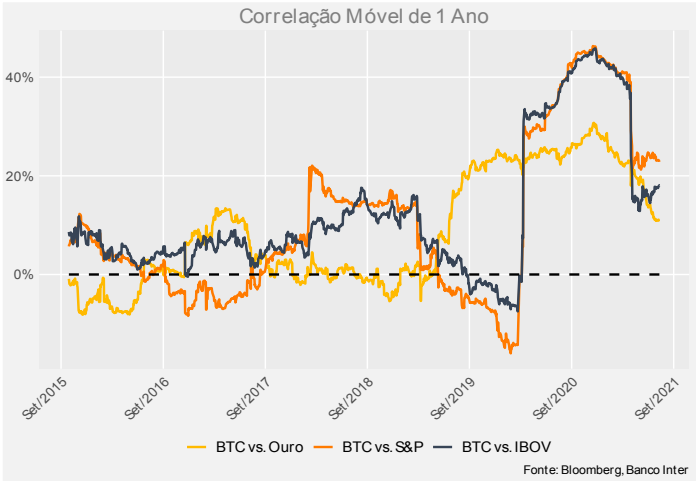
1. *Vitreo Cripto Metals Blend FIC FIM;*
2. *Vitreo Criptomoedas FIC FIM IE*;*
3. *Hashdex 20 Nasdaq Crypto Index FIC FIM (20/80 cripto e renda fixa);*
4. *Hashdex 40 Nasdaq Crypto Index FIC FIM* (40/80 cripto e renda fixa);*
5. *HASH11, ETF de criptomoedas da Hashdex;*
6. *QBTC11, ETF 100% Bitcoin.*

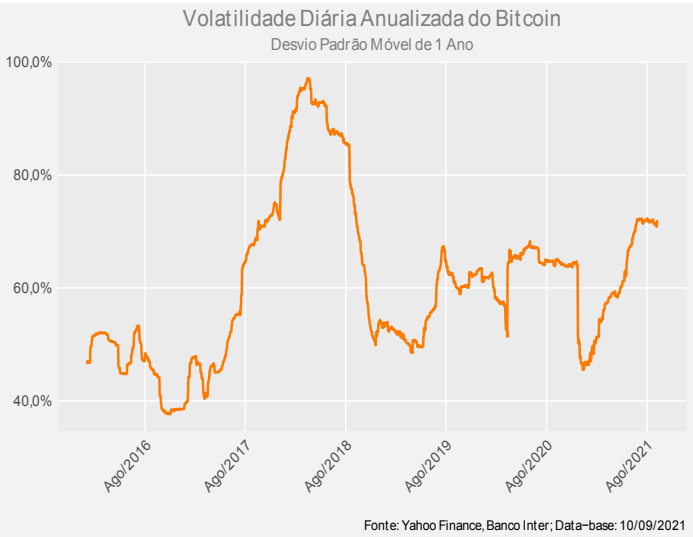
**somente para investidores qualificados*

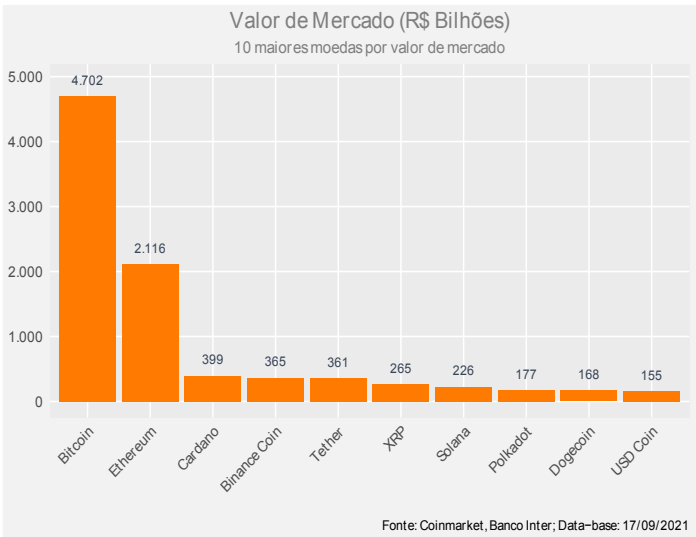

Bitcoin (BTC)
Retorno em US$ em 12 meses
500,0%
400,0%
300,0%
200,0%
100,0%
0,0%
331,3%
33,3%
Set/2020
Dez/2020
Mar/2021
Jun/2021
Set/2021
Bitcoin
S&P
Fonte: Yahoo Finance, Banco Inter; Data-base: 17/09/2021


Ethereum (ETH)
Retorno em US$ em 12 meses
800,0%
400,0%
0,0%
773,7%
33,3%
Set/2020
Dez/2020
Mar/2021
Jun/2021
Set/2021
Ethereum
S&P
Fonte: Yahoo Finance, Banco Inter; Data-base: 17/09/2021


Oferta Monetária de Bitcoin (Milhões)
Oferta Máxima (21 Milhões)
20
15
10
5
0
1,0
7,0
11,5
14,4
16,5
17,9
18,8
Set/09
Set/11
Set/13
Set/15
Set/17
Set/19
Set/21
Fonte: Coinmetrics, Banco Inter


Correlação Móvel de 1 Ano
40%
20%
0%
Set/2015
Set/2016
Set/2017
Set/2018
Set/2019
Set/2020
Set/2021
BTC vs. Ouro
BTC vs. S&P
BTC vs. IBOV
Fonte: Bloomberg, Banco Inter


Volatilidade Diária Anualizada do Bitcoin
Desvio Padrão Móvel de 1 Ano
100,0%
80,0%
60,0%
40,0%
Ago/2016
Ago/2017
Ago/2018
Ago/2019
Ago/2020
Ago/2021
Fonte: Yahoo Finance, Banco Inter; Data-base: 10/09/2021


Valor de Mercado (R$ Bilhões)
10 maiores moedas por valor de mercado
5.000
4.000
3.000
2.000
1.000
0
4.702
2.116
399
365
361
265
226
177
168
155
Bitcoin
Ethereum
Cardano
Binance Coin
Tether
XRP
Solana
Polkadot
Dogecoin
USD Coin
Fonte: Coinmarket, Banco Inter; Data-base: 17/09/2021

Disclaimer

Este material foi preparado pelo Banco Inter S.A. e destina-se à informação de investidores, não constituindo oferta de compra ou venda de títulos ou valores mobiliários. Os ativos discutidos neste relatório podem não ser adequados para todos os investidores.
Este material não leva em consideração os objetivos de investimento, a situação financeira e as necessidades específicas de qualquer investidor em particular. Aqueles que desejem adquirir ou negociar os ativos objeto de análise neste material devem obter as informações pertinentes para formarem sua própria convicção sobre o investimento.
As decisões de investimento devem ser realizadas pelo próprio investidor. É recomendada a leitura dos prospectos, regulamentos, editais e demais documentos descritivos dos ativos antes de investir, com especial atenção ao detalhamento do risco do investimento. Investimentos nos mercados financeiros e de capitais estão sujeitos a riscos de perda superior ao capital investido. A rentabilidade obtida no passado não representa garantia de resultados futuros.
As informações, opiniões e estimativas contidas no presente material foram obtidas de fontes consideradas confiáveis pelo Banco Inter S.A. e este relatório foi preparado de maneira independente.
Em que pese tenham sido tomadas todas as medidas razoáveis para assegurar a veracidade das informações aqui contidas, nenhuma garantia é firmada pelo Banco Inter S.A. ou pelos analistas responsáveis quanto à correção, precisão e integridade de tais informações, ou quanto ao fato de serem completas. As informações, opiniões, estimativas e projeções contidas neste documento referem-se à data em que o presente material foi disponibilizado e estão sujeitas a mudanças, não implicando necessariamente na obrigação de qualquer comunicação, atualização ou revisão do presente material.
O analista de valores mobiliários responsável por este relatório declara que as recomendações e análises refletem única e exclusivamente as suas opiniões pessoais e que foram elaboradas de forma independente, inclusive em relação à pessoa jurídica à qual está vinculado, podendo, inclusive, divergir com a de outros analistas do Banco Inter S.A., ou ainda com a de opinião de seus acionistas, instituições controladas, coligadas e sob controle comum (em conjunto, “Inter”).
Nos termos da regulamentação em vigor, a área de research do Inter é segregada fisicamente de outras atividades que podem ensejar potenciais conflitos de interesses.
O Banco Inter S.A. e as demais empresas do Inter poderão, respeitadas as previsões regulamentares, vender e comprar em nome próprio, de clientes e/ou via fundos de investimentos sob gestão, valores mobiliários objeto do presente relatório, bem como poderão recomendá-los aos seus clientes, distribuí-los, prestar serviços ao emissor do valor mobiliário objeto do relatório que enseje em pagamento de remuneração ao Banco Inter S.A. ou a empresas do Inter, ou, ainda, na hipótese do presente relatório ter como objeto fundo de investimento, originar ativos que serão adquiridos pelo veículo objeto do presente relatório.
O Banco Inter S.A. e outras empresas do Inter podem ter interesse financeiro e/ou comercial em relação ao emissor ou aos valores mobiliários objeto do relatório de análise, ou até mesmo participação societária em emissores objeto do presente relatório, suas controladas, controladores, coligadas e/ou sociedades sob controle comum.
Ademais, o analista responsável pelo presente relatório declara que:
(i) os analistas de valores mobiliários envolvidos na elaboração do presente relatório não possuem vínculo com pessoa natural que trabalha para o emissor objeto do relatório;
(ii) os analistas de valores mobiliários envolvidos na elaboração, seus cônjuges ou companheiros, são direta ou indiretamente, em nome próprio ou de terceiros, titulares de valores mobiliários objeto do relatório de análise;
(iii) os analistas de valores mobiliários envolvidos na elaboração, seus cônjuges ou companheiros, são direta ou indiretamente envolvidos na aquisição, alienação e/ou intermediação dos valores mobiliários objeto do relatório;
(iv) os analistas de valores mobiliários envolvidos na elaboração do relatório, seus cônjuges ou companheiros, possuem direta ou indiretamente, interesse financeiro em relação ao emissor objeto do relatório de análise; e
(v) a sua remuneração e dos analistas de valores mobiliários envolvidos na elaboração do presente relatório é direta ou indiretamente, influenciada pelas receitas provenientes dos negócios e operações financeiras realizadas pelo Banco Inter.
Por sua vez, ante a ativo objeto de análise, o Inter declara que:
(i) não possui participações societárias relevantes no emissor objeto do relatório de análise ou em que o emissor objeto do relatório de análise, suas controladas, seus controladores ou sociedades sob controle comum tenham participações relevantes nos analistas de valores mobiliários pessoa jurídica, suas controladas, seus controladores ou sociedades sob controle comum;
(ii) possui interesses financeiros e comerciais relevantes em relação ao emissor ou aos valores mobiliários objeto do relatório de análise;
(iii) não está envolvidas na aquisição, alienação ou intermediação dos valores mobiliários objeto do relatório de análise; e
(iv) não recebe remuneração por outros serviços prestados para o emissor objeto do relatório de análise ou pessoas a ele ligadas.
Para maiores informações, é recomendável que os destinatários consultem a Resolução CVM/20, de 25 de fevereiro de 2021, e, também, o Código de Conduta da Apimec para o Analista de Valores Mobiliários.