



2FA

❶ (abreviatura de “two-factor authentication”, ou “autenticação de dois fatores”): o uso de uma outra maneira (normalmente uma senha descartável, mas às vezes pode ser impressão digital, reconhecimento de face, etc.) para identificar o usuário além do tradicional nome e senha (que seriam o “primeiro fator de autenticação”). *Veja também:* ➤ [senha descartável](#).

📖 *“Praticamente toda corretora hoje em dia suporta 2FA, ative para não ser ‘hackeado!’”*

airdrop

❶ distribuição gratuita de unidades de uma determinada criptomoeda ou token, comumente utilizada como estratégia de marketing para aumentar a adoção, conscientização e engajamento de um token recém lançado.

airgapped

❶ (idiomaticamente, “apartado pela lacuna de ar”) diz-se de um computador (uma carteira em hardware, por exemplo) totalmente isolado, sem nenhuma forma de conexão com a internet, nem com nenhum outro computador.

alfaçar

❶ (gíria) o ato de vender ativos prematuramente ou contra os próprios interesses devido a ansiedade, exaustão emocional ou pânico causado por um evento dramático recente (tipicamente, uma queda abrupta no preço), sem considerar a possibilidade de uma recuperação a médio ou longo prazo. *Veja também:* ➤ [mão de alface](#).

algoritmo

❶ procedimento explicitando minuciosamente e detalhadamente como realizar uma determinada tarefa (em geral, a realização de um cálculo, obtenção de um resultado, etc.)

📖 *As linguagens de programação são diferentes maneiras de expressar algoritmos em forma escrita.*

📖 *O algoritmo de prova de trabalho do Bitcoin é o SHA256d.*

all time high

❶ *mesmo que:* ➤ [alta histórica](#);



alta histórica

❶ (em inglês, “*all time high*”, frequentemente abreviado “ATH”): o maior preço (relativo a uma moeda nacional, tal como reais ou dólares) que se tem notícia de um ativo jamais ter tido em alguma corretora.

altura

❶ de um bloco dentro de um *blockchain*, quantos blocos é preciso retroceder, seguindo a cadeia de antecessores, até se chegar ao bloco gênese. Análogo ao “número da edição” de uma “revista” ou “diário oficial”, exceto que a numeração começa em zero.

AML

❶ (sigla em inglês de “Anti-Money Laundering”, ou “anti-lavagem de dinheiro”): conjunto de medidas que as corretoras e agentes do mercado financeiro tradicional são cobradas pelo governo a adotar para identificar suspeitas de lavagem de dinheiro e reportá-las às autoridades.

alt

❶ *contração de:* • altcoin.

📖 “*Aquele cara virou o louco das alts*” (passou a só querer negociar altcoins)

altcoin

❶ (contração de “*alternative coin*”; “moeda alternativa”, em Português) termo genérico para se referir a outras criptomoedas que não sejam Bitcoin.

análise fundamentalista

❶ método de avaliação de um ativo que envolve a análise detalhada de fatores econômicos, financeiros, qualitativos e quantitativos. No caso de ações, por exemplo, busca entender a saúde financeira da empresa, suas perspectivas de crescimento, a qualidade da sua gestão, o cenário da indústria em que está inserida, etc. No contexto das criptomoedas, avalia o código-fonte já publicado do projeto, a solidez da tecnologia, a qualidade da equipe de desenvolvimento, adoção atual da criptomoeda e o crescimento esperado, entre outros. *Contraste com:* • análise técnica.

análise técnica

❶ Método de avaliação amplamente usado nos mercados de ações, futuros, criptomoedas, etc., que busca prever a direção futura dos preços de determinados ativos financeiros através do estudo de dados de mercado passados, principalmente preço e volume, partindo da premissa de que se movem em tendências identificáveis

de curto, médio e longo prazo. *Contraste com:* • análise fundamentalista.

armazenamento frio

❶ ato de armazenar chaves privadas ou informações altamente sigilosas em dispositivos que permanecem a maior parte do tempo desligados, ou cujo acesso e uso requer uma intervenção física (possivelmente demorada) do seu guardião, ou que nem sequer sejam eletrônicos. ❷ o local ou meio físico onde esse armazenamento é feito. ❸ sinônimo informal, mas tecnicamente incorreto, para: • carteira em hardware.

armazenamento quente

❶ ato de armazenar chaves privadas ou informações altamente sensíveis em um computador conectado constantemente à internet, para que as assinaturas digitais e/ou transações de criptomoeda possam ser feitas instantaneamente quando requisitadas.

📖 *A maioria das corretoras tem uma carteira quente para os saques do dia-a-dia e outra em armazenamento frio com o grosso dos fundos depositados, recarregando uma em função da outra de acordo com suas políticas de gestão de riscos.*

ASIC

❶ (sigla de “Application-Specific Integrated Circuit”, ou “Circuito Integrado para Aplicação Específica”) um “chip” (circuito integrado) intencionalmente projetado e fabricado para realizar alguma tarefa de forma extremamente eficiente (seja em velocidade, seja em baixo consumo de energia, ou ambos).

📖 *Os ASICs dominaram a indústria de mineração do Bitcoin e de várias outras criptomoedas.*

assinatura digital

❶ procedimento de cálculo oriundo da disciplina de criptografia que combina uma mensagem (tipicamente uma transação) e uma chave privada, resultando em um número que serve como “testemunha”, “selo” ou “código verificador” de que aquela exata chave privada e aquele exato documento foram combinados. Assinaturas digitais são amplamente utilizadas como meio de autorizar transferências de criptomoedas. ❷ o resultado desse cálculo para uma chave privada e mensagem específicas.

📖 *Não confunda assinatura digital com assinatura manuscrita digitalizada!*



📖 *Tem muita gente tentando emplacar a ideia que uma mera senha é uma “assinatura digital”! Não caia nessa falácia. Se não é calculada em função de um documento ou mensagem, e específica para este, não é uma assinatura digital!*

ATH

① sigla de “All Time High”, veja: [alta histórica](#);

ativo

① algum bem ou direito cuja posse ou uso pode potencialmente trazer benefícios, dinheiro ou tende a aumentar o patrimônio.

📖 *Para um motorista de Uber, seu carro é seu maior ativo.*

ativo virtual

① definida na Lei 14.478 de 21/12/2022 como a representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento que não sejam moedas nacionais ou estrangeiras, moeda eletrônica, pontos de fidelidade, nem valores mobiliários. Entende-se que as criptomoedas/criptoativos se encaixam nessa definição.

ativo financeiro

① Um ativo intangível cujo valor é oriundo de um direito contratual ou de propriedade.

atomic swap

① mesmo que: [troca atômica](#).

atômico

① em ciência da computação, diz-se de uma operação dita “indivisível”, em que todas as suas eventuais sub-partes são ou executadas com sucesso, ou nenhuma delas é executada em absoluto, de forma a nunca deixar resíduos, inconsistências, nem resultados parciais ou incompletos.

📖 *Uma função pouco apreciada das corretoras é garantir atomicidade: quando você compra, seu saldo em criptomoedas aumenta e seu saldo em fiat diminui (e vice-versa ao vender). O problema do P2P (e do “comércio eletrônico em geral”) é justamente a falta de atomicidade: a contraparte pode não cumprir sua parte, aí você manda seu dinheiro e não recebe seu produto.*

auditabilidade universal

① propriedade da maioria das criptomoedas, bem como de muitas soluções baseadas em *blockchains*/DLTs, em que todos os participantes (e às vezes até observadores



externos) podem conferir independentemente o correto funcionamento e operação do sistema a partir do seu histórico de transações público. Juntamente com a contabilização perfeita, é uma das principais razões por trás do grande interesse nessa tecnologia.

auto-custódia

❶ situação em que o proprietário legal ou moral detém controle total e exclusivo das chaves privadas que permitem a transferência de suas criptomoedas para outros endereços.

📖 *Praticar a auto-custódia maximiza a autonomia e privacidade, mas requer manjar muito bem de segurança cibernética, pois exige maior responsabilidade e cuidado para proteger as chaves privadas contra perda ou roubo.*

base16

❶ mesmo que: [hexadecimal](#);

base58

❶ sistema de numeração baseado em 58 dígitos consistindo de números, letras maiúsculas e minúsculas (consideradas diferentes), mas excluindo o numeral zero e a letra "O" maiúscula (por serem fáceis de confundir um com o outro), bem como a letra "L" minúscula e a letra "I" maiúscula (pela mesma razão). Embora ainda amplamente adotado tanto pelo Bitcoin quanto por várias outras criptomoedas para composição de endereços, está sendo gradualmente substituído pelo sistema Bech32.

📖 *Na rede Bitcoin principal (mainnet), os endereços Base58 sempre começam com "1" ou "3". Já na testnet, começam com "2", "m" ou "n". Alguns golpistas se aproveitam disso para vender bitcoins da testnet, que não têm valor de revenda, para "bicoiners" incautos.*

bear market

❶ momento de pessimismo e desânimo no mercado devido à queda, ou expectativa de queda, nos preços dos ativos, por um período de tempo relativamente longo.

📖 *Conta a lenda que o termo "bear market" (mercado dos ursos) advém da maneira como os ursos atacam, empurrando suas vítimas para baixo, contra o chão.*

bech32

❶ sistema de numeração baseado em 32 dígitos consistindo de 23 letras (maiúsculas são consideradas idênticas às minúsculas) e 9 números, usado em um novo formato de endereços de recebimento da rede Bitcoin (introduzido na atualização "segwit" da rede



Bitcoin em 2017) e também adotado por várias outras criptomoedas dele derivadas. O bech32 incorpora um código corretor de erros que permite detectar e em muitos casos corrigir erros de transcrição.

📖 *Na rede Bitcoin principal, os endereços Bech32 sempre começam com “bc 1” e os da testnet com “tb 1”.*

bech32m

❶ evolução do sistema de endereçamento bech32 para corrigir uma fraqueza descoberta no código corretor de erros após sua introdução.

BIP

❶ (sigla de “Bitcoin Improvement Proposal”, ou “Proposta de Melhoria do Bitcoin”) série de documentos técnicos detalhando minuciosamente propostas para novos recursos e melhorias no Bitcoin ou em seu entorno, bem como seus prós e contras, para debate entre os desenvolvedores e servindo de guia para os que forem implementá-la. Algumas propostas não pegam tração, mas algumas são implementadas, resultando em uma nova versão do bitcoin ou de algum dos programas/sistemas adjuntos. ❷ (juntamente com o número, p. ex., “BIP44”) um documento específico dentro dessa série.

📖 *Tem uma ideia nova para o Bitcoin? Escreve um BIP e circula entre a comunidade.*

bit

❶ (contração de “binary digit”, ou “dígito binário” em Português) em Ciência da Computação, a menor unidade de armazenamento de informação possível, capaz de discriminar entre dois estados claramente distintos, tais como “ligado” versus “desligado”, “aceso” versus “apagado”, tradicionalmente representados de forma mais abstrata pelos dígitos 0 (zero) e 1 (um). Todo e qualquer tipo de informação no Universo teoricamente pode ser representada como uma sequência (potencialmente longa) de bits. ❷ sinônimo (não muito popular) para a unidade de conta “microbitcoin”.

bitcoin

❶ (tradicionalmente com inicial maiúscula) a primeira criptomoeda da história, criada em 2008/2009 por Satoshi Nakamoto, e que deu origem à toda a área de criptomoedas descentralizadas com participantes equipotentes, inventora do *blockchain* com contabilização perfeita e auditabilidade universal, pioneira na adoção da prova de trabalho como critério de desempate; ❷ (tradicionalmente com inicial minúscula; símbolo: ₿) a unidade de conta desta criptomoeda; ❸ o preço de uma unidade de bitcoin relativo a alguma moeda nacional; ❹ sinônimo informal para “rede bitcoin”; ❺ o programa de computador que implementa todo esse sistema;



- 📖 *Você é dos que dizem “o bitcoin” ou dos que dizem “a bitcoin”?*
- 📖 *Até hoje não se sabe quem realmente é, ou foi, o inventor do Bitcoin;*
- 📖 *O Bitcoin caiu um pouco hoje. Ou melhor, quem caiu foi o preço do Bitcoin, a rede Bitcoin continua de pé!*

OS VÁRIOS SIGNIFICADOS DE “BITCOIN”

O Bitcoin é, na verdade, um programa aplicativo de computador (um “app”, em uma simplificação talvez exagerada). Quando várias pessoas (na condição de voluntárias sem vínculo formal) o executam em seus computadores, eles se encontram através da internet e criam a chamada “rede Bitcoin”. Esta rede atua como um misto de “casa da moeda” e “cartório”, registrando a emissão e circulação de unidades monetárias (também chamadas de “bitcoin”, mas com inicial minúscula).

E tem mais: ao redor da “rede Bitcoin” existem os vários membros do “ecossistema Bitcoin” (empresas, tipicamente) que oferecem uma ampla variedade de serviços para os usuários finais. Entre eles, destacam-se as “corretoras”, que facilitam o processo de compra e venda de bitcoins através de moedas nacionais, como reais brasileiros, dólares ou euros. Disso decorre que o “preço do Bitcoin” é oriundo da tensão entre oferta e demanda nas corretoras, e não da rede Bitcoin em si.

Isso acrescenta ainda outro significado à palavra: muita gente usa o termo “bitcoin” para se referir ao seu preço de mercado, e não à rede de voluntários ou ao programa de computador. Quando vemos uma manchete dizendo, por exemplo, “bitcoin teve queda”, o que realmente está se querendo dizer é que “O preço do bitcoin teve uma queda”, não que a rede “caiu” ou “saiu do ar”. Perguntar “como está o bitcoin hoje?” é uma forma abreviada de dizer “o preço do bitcoin subiu, caiu ou permanece estável?”

Em suma, “bitcoin” pode ser o programa de computador, a rede de voluntários, o ecossistema de empresas ao redor da rede principal, ou seu preço. Cada significado tem uma história e comunidade próprias e, como às vezes um mesmo texto usa vários dos diferentes significados da palavra, é necessário inferir o significado correto através do contexto.

Por fim, usamos neste texto o Bitcoin como exemplo, mas a mesma ideia se aplica a outras criptomoedas, tais como Ethereum, Litecoin, Monero, etc.

blockchain

❶ um histórico sequencial de transações ou registros de dados/eventos agrupados em blocos (análogo a “edições” de uma revista ou “diário oficial”) que empregam criptografia para criar uma cadeia de verificação de integridade desde a primeira edição até a mais recente, atuando como registro oficial e autoridade final sobre se uma determinada transação ou evento de fato ocorreu ou não. ❷ O histórico de



transações de uma criptomoeda específica (p. ex., “o blockchain do Bitcoin”). ③ A abordagem geral de usar sistemas computacionais baseados em blockchains para registrar fatos, eventos ou transações.

📖 *Se a transação não consta no blockchain, ela não aconteceu!*

📖 *Blockchains só promovem a transparência universal se forem públicos.*

BLOCKCHAINS ATRAVÉS DA ANALOGIA DOS DIÁRIOS OFICIAIS

Uma analogia que facilita entender como os blockchains funcionam é compará-los ao Diário Oficial da União (DOU): uma lei ou ato do governo só vale se publicada nele. Cada edição (no blockchain, chamam-se blocos) reúne diversos atos, decretos ou leis (transações) de diversos órgãos do governo (os usuários). Esta é a função do blockchain: oficializar as transações.

Uma coisa que os blockchains têm, mas os diários oficiais não, é um sistema embutido de verificação de integridade: a partir do conteúdo de todas as transações em um bloco (“block”, em inglês), calcula-se um número que age como seu identificador universalmente único. Além disso, cada novo bloco inclui o identificador do anterior, formando uma sequência encadeada (daí o termo “chain”). Se for feita qualquer alteração no conteúdo de qualquer bloco, por menor que seja, os identificadores mudam, “quebrando a cadeia” e permitindo que se detecte que não está correto.

Isso parece pouco importante no mundo real das publicações impressas, pois, em caso de suspeita de adulteração, pode-se conferir diretamente com a Imprensa Oficial. Contudo, é essencial no mundo da internet porque o blockchain é feito para operar sem intervenção humana, de forma que, essa conferência precisa ser feita matematicamente pelos computadores. Sem ela, haveria mil oportunidades de adulteração, pois é fácil alterar documentos digitais sem deixar evidências periciáveis. Com ela, é possível tanto convencer-se, quanto provar para observadores externos, que o bloco recebido é idêntico bit a bit ao publicado – ou seja, que não houve adulteração.

O DOU é criado, compilado, editado e publicado por uma entidade centralizada, a Imprensa Oficial. Da mesma forma, existem blockchains centralizados. Contudo, onde os blockchains brilham, mesmo, é em situações descentralizadas, onde muitos participantes atuam de forma colaborativa e igualitária.

Para visualizar esse cenário, imaginemos que, ao invés do DOU, todos os órgãos do governo mandassem seus atos (transações) para um conjunto de voluntários, onde cada um compilaria independentemente sua própria versão da próxima edição (é natural que as várias versões sejam ligeiramente diferentes apesar de em grande medida semelhantes, pois diferentes empresas podem receber as transações em diferentes ordens).

No final de cada dia é realizado um sorteio e o voluntário que ganha tem sua versão declarada como “oficial”. Os perdedores conferem que a versão oficial está rigorosamente



de acordo com as regras e, se sim, descartam suas versões e começam a trabalhar na próxima rodada; se não, a versão transgressora é descartada e um novo sorteio é realizado.

É mais ou menos assim que os blockchains de muitas criptomoedas, como o Bitcoin, funcionam. A diferença é que o processo de escolha da versão ganhadora também é auditável: é possível provar que o sorteio deu mesmo aquele resultado e que foi feito de forma justa, imparcial e proporcional à quantidade de esforço despendido. E como todos os participantes conferem a versão oficial antes de aceitá-la como tal, isso viabiliza todos os concorrentes serem iguais, sem nenhum ser o chefe. Ou seja, o sistema funciona de forma descentralizada, sem a necessidade de um coordenador central.

Imagine ainda que os atos que são oficializados nesse “diário oficial” seja a criação de novas unidades monetárias (“Estejam aqui criados 50 novas moedas, entregues à entidade X”) e sua circulação, na forma da transferência entre os participantes (“X transfere 5 de suas 50 moedas para Y, ficando com um saldo de 45”; “Y transfere 1 moeda para Z, ficando com um saldo de 4”). Tem-se, então, uma moeda criada por sobre um diário oficial, um “dinheiro virtual” – exatamente o que o Bitcoin faz. E com a vantagem de ser continuamente auditado, resultando em uma “contabilização perfeita” em que nenhuma unidade monetária jamais é perdida, nem fabricada fora das regras.

Nenhuma analogia é perfeita, e essa não seria exceção: há muito mais detalhes sobre o funcionamento do Bitcoin em particular e sobre as criptomoedas em geral que ela não abarca. Mesmo assim, serve bem para ilustrar a essência do que é um **blockchain**: um histórico de transações construído a muitas mãos; e uma criptomoeda: a criação e circulação de unidades monetárias registrada nesse **blockchain**.

bloco

❶ um lote de transações dentro de um *blockchain*, juntamente informações que permitem verificar a integridade dos dados nele contido e encaixá-lo corretamente na sequência. Vagamente análogo à “uma edição” de uma “revista” ou “diário oficial”.

bloco gênese

❶ o bloco inicial que dá partida a uma criptomoeda ou *blockchain*, vagamente semelhante à “edição inaugural” de uma revista, servindo de ponto de partida para o histórico de transações. Por definição, tem altura igual a zero e é o único que não tem antecessor.

📖 *O bloco gênese do Bitcoin é famoso por conter uma mensagem com o texto de uma das manchetes da primeira página da edição de 3 de janeiro de 2009 de um jornal britânico.*

brain wallet

❶ *mesmo que:*  carteira mental;



BRL

❶ abreviatura de Reais Brasileiros (“Brazilian Real”), a moeda nacional do Brasil, segundo o padrão ISO 4217;

BTC

❶ abreviatura de bitcoin, a unidade de conta. Apesar de tradicional e popular, essa abreviatura conflita com as regras do padrão ISO 4217. *Contraste com:* • XBT;

bull market

❶ momento de otimismo e euforia no mercado devido à alta, ou expectativa de alta, nos preços dos ativos, por um período de tempo relativamente longo.

📖 *Conta a lenda que o termo “bull market” (mercado dos touros) advém da maneira como os touros atacam, jogando suas vítimas para cima.*

byte

❶ (pronuncia-se “báit”) unidade de medida de armazenamento de informação corresponde a 8 bits, capaz de armazenar um caractere (letra/número/sinal de pontuação) dos sistemas de escrita ocidentais (alfabeto romano, etc.).

capitalização de mercado

❶ (“market capitalization”, em inglês, frequentemente abreviado para “market cap”) número resultante da multiplicação entre a quantidade total de unidades monetárias circulantes vezes seu preço unitário nas corretoras. É uma métrica muito popular no mercado financeiro para dar uma ideia grosseira do “tamanho do mercado” de um determinado ativo, mas há quem critique seu uso no âmbito das criptomoedas por dar resultados inflados devido a variação de preço extrema que muitas criptomoedas tiveram ao longo de suas histórias.

📖 *No pico de 2019, o market cap do Bitcoin passou de 1 trilhão de dólares.*

carteira

❶ um aplicativo ou programa de computador que cria, armazena e gere chaves privadas, calcula endereços e saldos, e permite realizar transferências de criptomoedas.

❷ sinônimo (informal e arcaico) para “endereço”.

📖 *Muitos usuários da “velha guarda” chamam “endereço” de “carteira” porque antigamente os aplicativos de carteira só geravam um único endereço. Hoje em dia, eles geram vários, evidenciando a distinção entre os conceitos.*



carteira de papel

❶ (“*paper wallet*”) uma folha de papel onde se escreve ou imprime uma chave privada e seu endereço correspondente, em forma textual e, frequentemente, também na forma de códigos QR.

📖 *Carteiras de papel são imunes a ataques cibernéticos, mas há o risco de elas serem perdidas ou achadas por outras pessoas que não seus legítimos donos.*

carteira mental

❶ (“*brain wallet*”) prática de memorizar a chave privada, ou algum precursor dela, em geral sem guardar nenhuma cópia dela em lugar nenhum.

📖 *Se bem escolhidas, carteiras mentais podem ser seguras contra quase tudo, exceto talvez tortura e Alzheimer.*

carteira em hardware

❶ (“*hardware wallet*”) aparelho especializado com a finalidade única de criar/gerir chaves privadas e assinar transações de redes de criptomoedas de forma apartada dos computadores principais de propósito geral do usuário (notebook, celular, etc.), oferecendo uma das melhores combinações entre segurança, conveniência e facilidade de uso.

📖 *Trezor, KeepKey, Ledger e Coldcard são algumas das mais famosas marcas de carteiras em hardware!*

cex

❶ (abreviatura de “Centralized Exchange”, ou “corretora centralizada” em Português) plataforma de negociação de criptoativos que opera através de um intermediário, distinto das redes dos criptoativos, que centraliza todas operações, e no qual é preciso confiar implicitamente que sempre agirá com lisura e jamais sucumbirá a ataques ou fraudes. As CEXs têm a vantagem de permitirem negociações muito rápidas e costumam ter interfaces de usuário mais fáceis, mais serviços ao cliente e mais opções de negociação. *Veja também:* ➤ [corretora](#).

📖 *“Se tem CNPJ, é CEX – convença-me do contrário!”*

chave privada

❶ dado sigiloso (normalmente um número inteiro grande) que confere aos seus detentores o poder de realizar transferências de criptomoedas (ou seja, que os torna “donos” delas) e, de forma mais genérica, criar assinaturas digitais que atestam a integridade de documentos digitais. *Contraste com:* ➤ [semente](#).



- 📖 *Se as chaves privadas vazarem, suas criptomoedas poderão ser roubadas!*
- 📖 *É essencial não perder as chaves privadas; sem elas, não há como mover os fundos.*
- 📖 *Uma característica essencial das chaves privadas é que calculá-las a partir das suas chaves públicas correspondentes é impraticável (apesar de teoricamente possível, leva milênios mesmo se pudéssemos alistar todos os computadores do mundo só para essa tarefa), tornando possível que o agente que confere uma assinatura digital possa apenas auditar a validade de uma assinatura, mas não gerar uma nova assinatura válida.*

chave pública

- ❶ um ou mais números calculados em função das respectivas chaves privadas. São tipicamente incluídas dos *scripts* e contratos inteligentes que, por sua vez, dão origem aos endereços visíveis pelos usuários finais e são internamente usadas no processo de conferência da validade das assinaturas digitais que autorizam a efetivação das transações.
- 📖 *Apesar de essenciais no processo de verificação de assinaturas digitais, quase nenhuma carteira mostra explicitamente as chaves públicas, mesmo não havendo problema nenhum em fazê-lo.*

código aberto

- ❶ ampla classe de regimes de licenciamento de software em que o código-fonte dos programas de computador (onde as ideias por trás do funcionamento dos programas são expressas na forma de mais fácil compreensão) são disponibilizados, em geral gratuitamente, para que possam ser estudados, copiados, e executados independentemente dos seus autores originais.
- 📖 *O Bitcoin, Ethereum e a maioria das principais criptomoedas são disponibilizadas sob licenças de código aberto, permitindo que seu funcionamento interno seja minuciosamente auditado.*

coinbase

- ❶ (sem tradução amplamente aceita em Português) transação inicial de todo bloco na rede bitcoin (e derivadas), onde a recompensa do minerador é registrada e as novas unidades monetárias criadas são colocadas em circulação. ❷ (com a inicial maiúscula, apesar do logotipo usar inicial minúscula) nome de uma famosa corretora de criptomoedas americana.

cold storage

❶ mesmo que: • armazenamento frio;

cold wallet

❶ mesmo que: • armazenamento frio;

computabilidade universal

❶ (também conhecida como “completude de Turing”, ou “Turing-completeness”, em inglês) capacidade de um computador real ou virtual, linguagem de programação ou modelo de computabilidade, de computar tudo que é teoricamente possível ser computado dentro das limitações de tempo e armazenamento. Na prática, significa que o sistema pode tratar problemas e/ou regras de negócios arbitrariamente complexas.

📖 *É justamente o fato da EVM do Ethereum ser capaz de computabilidade universal que viabiliza a “inteligência” dos “contratos inteligentes” e seu uso como “dinheiro programável”, dando origem a tantas aplicações diferentes.*

📖 *Para evitar os bugs e problemas de segurança inerentes à computabilidade universal, algumas criptomoedas, como o Bitcoin, deliberadamente restringem seus engenhos de script para não serem capazes de computabilidade universal.*

📖 *A computabilidade universal é um conceito oriundo de um ramo da Ciência da Computação Teórica chamado Teoria da Computabilidade, que estuda, entre outras coisas, o que um computador minimamente precisa ter para ser capaz de computar.*

confirmações

❶ a quantidade de blocos desde aquele onde uma determinada transação foi publicada até o bloco mais recente. Ou seja, quando uma transação é inicialmente incluída em um bloco, diz-se que ela tem “uma confirmação” (o bloco onde a transação foi publicada é o mais recente). Quando o próximo bloco sai, ela tem “duas confirmações” (o bloco onde a transação foi publicada é o segundo mais recente), e assim sucessivamente. Na rede Bitcoin e em várias outras, uma transação é considerada “plenamente confirmada” quando ela tem pelo menos seis confirmações.

contabilização perfeita

❶ propriedade da maioria das criptomoedas, bem como de muitas soluções baseadas em *blockchains*/DLTs, em que os cálculos referentes à criação e circulação das unidades monetárias sempre estão absolutamente corretos bloco a bloco, de acordo com as regras da criptomoeda. Juntamente com a auditabilidade universal, é uma das principais razões por trás do grande interesse nessa tecnologia.

contrato inteligente

❶ um programa de computador contido em alguma rede de criptomoedas, capaz de "pagar e/ou ser pago" para executar ações de acordo com regras pré-definidas (vagamente análogo a "cumprir cláusulas" de um "contrato", daí o nome) de forma determinística: chegando sempre ao mesmo resultado independente de quando sejam executados ou qual nó exato da rede o executa.

- 📖 *A perspectiva estreita sobre contratos inteligentes é que eles não são contratos, no sentido jurídico do termo, nem tampouco inteligentes, no sentido em que as pessoas normalmente atribuem à palavra "inteligente".*
- 📖 *A perspectiva ampla sobre contratos inteligentes é que, mesmo sendo apenas programas de computador, eles executam vontades pré-acordadas entre partes, daí o termo "contrato".*
- 📖 *O adjetivo "smart" nos "smart contracts" que dizer apenas que eles são "programáveis", no sentido de "expressível na forma de um programa de computador".*
- 📖 *O resultado de um contrato inteligente não pode depender de fatores externos, como, por exemplo, um número aparecendo em um site ou uma API.*

CONTRATOS INTELIGENTES SÃO PROGRAMAS DE COMPUTADOR

O termo "contratos inteligentes" ("smart contracts", em inglês) causa muita confusão porque eles não são nem contratos, no sentido jurídico do termo, nem tampouco inteligentes. De fato, até o próprio inventor do Ethereum já expressou seu arrependimento por ter adotado esse termo, dizendo que melhor teria sido chamar de algo mais neutro, tal como "roteiros persistentes".



Na verdade, os contratos inteligentes são programas de computador, listas passo-a-passo de ações a serem tomadas quando certos eventos ocorrem – por exemplo, quando fundos são recebidos. Um exemplo simples de entender é o de uma loteria:

[Ao receber fundos:](#)



- Se a data de chegada deste pagamento for anterior à data do sorteio, acrescente esses fundos ao bolão e registre o endereço de origem na lista de apostadores.

- Caso contrário, sorteie aleatoriamente um apostador dentro da lista, pague 50% do bolão para ele e envie o restante para o endereço do dono da loteria.

(Os contratos inteligentes de verdade não são escritos em Português, e sim em uma linguagem de computador, muito mais detalhada e precisa.)

Vê-se daí que a analogia com um "contrato" até tem um certo sentido, porque essa lista de ações expressa as regras de funcionamento da empreitada, vagamente semelhante às "cláusulas" de um contrato da vida real.

Daí o entusiasmo com sistemas desse tipo: tem-se ampla versatilidade para criar "contratos inteligentes" que exprimem diversos tipos de "regras de negócio": loterias, jogos, captação de recursos, e muitos outros. Há, porém, algumas limitações cruciais; a maior delas é que o contrato precisa sempre dar exatamente o mesmo resultado quando executado sob condições idênticas, pois, sem isso, não seria possível auditar externa e independentemente que ele foi executado corretamente.

Por outro lado, também é justo afirmar que a analogia com um "contrato" falha sob inúmeros aspectos. As cláusulas de contratos jurídicos tradicionais são cumpridas (ou descumpridas!) por seres humanos; já os "contratos inteligentes" são executados pelos computadores – e, como tal, são cumpridos à risca: não há descumprimento em absoluto. Porém, caso o contrato não tenha previsto alguma coisa, ele dará um resultado inesperado que poderá desfavorecer algumas das partes – uma vez lançado, o contrato não pode ser mudado e não há nenhum tribunal ou processo para resolver potenciais disputas, erros, ou vícios que porventura tenham passado despercebidos.

Em suma, os "contratos inteligentes" são, na verdade, programas de computador que podem pagar e serem pagos nas unidades monetárias nativas da plataforma onde são publicados, sendo executados de forma totalmente automática por uma rede de computadores global e descentralizada.

corretora

① empresa especializada na intermediação de negociações (compra e venda) de criptomoedas, agregando segurança operacional e jurídica nas transações, custódia e possivelmente vários outros serviços, oferecidos tipicamente através de um aplicativo e/ou *site* na internet acessível pelo navegador.

corretora descentralizada

① (tipicamente abreviado como "dex", contração de "decentralized exchange") plataforma de negociação de criptoativos em que as negociações ocorrem diretamente entre os usuários através de contratos inteligentes em uma *blockchain*, dispensando uma autoridade central.



criptoativos

❶ o uso de criptomoedas de forma análoga a ativos financeiros, cuja posse ou negociação pode ser usada para trazer retornos financeiros ou outros benefícios ao seu detentor.

criptografia

❶ subdisciplina da Matemática e Ciência da Computação que estuda como manter integridade e confidencialidade em sistemas de armazenamento, processamento ou transmissão mesmo em face de adversários que estejam ativamente tentando interceptar ou adulterar os dados, provendo a base essencial para a existência e funcionamento das criptomoedas (daí o sufixo “cripto” em “criptomoedas”).

“CRIPTOMOEDAS” VS “MOEDAS CRIPTOGRAFADAS”

Apesar da disciplina da Criptografia ter diversas aplicações, o termo “criptografado” normalmente é usado com o significado estreito de “sigilo”: tornar uma mensagem incompreensível para algum intermediário que não tenha a “chave” correta para “decifrá-la”.

Por isso, o termo “moeda criptografada” soa inapropriado, pois a maioria das criptomoedas (tal como Bitcoin e suas derivadas, Ethereum, etc.) preza por ter seus históricos de transação totalmente abertos para que se possa auditar independentemente seu correto funcionamento, podendo inclusive rastrear os endereços de origem e destino em cada transação e os valores envolvidos.

De fato, o sufixo “cripto” no termo “criptomoedas” se refere muito mais ao uso da criptografia para verificação de integridade e autorização: qualquer tentativa de adulterar o histórico de transações ou mover uma unidade de criptomoeda que não lhe pertença é prontamente detectado e rejeitado.

Há criptomoedas, como Monero ou ZCash, em que a criptografia é usada no sentido tradicional de esconder dados, inclusive os valores e endereços de origem e destino. Nesse caso, chamá-las de “moedas criptografadas” seria até apropriado. Mas, como elas não são nem as mais usadas, nem as mais conhecidas, o potencial de confusão com as demais criptomoedas é considerável, especialmente entre os leigos e novatos.

Para não reforçar essa confusão, é preferível usar o termo “criptomoeda” e evitar o termo “moeda criptografada”.

criptografia fim-a-fim

❶ uso de criptografia em que os usuários finais realizam as operações criptográficas, impossibilitando trapaças por parte dos operadores, intermediários ou centralizadores por onde as mensagens ou transações passam.



criptomoeda

❶ sistema de contabilização de criação e circulação de valores que emprega criptografia fim-a-fim e *blockchains* para obter características (resistência a adulteração, auditabilidade universal independente, descentralização, contabilização perfeita) que não são possíveis de outra forma.

PODEM AS CRIPTOMOEDAS SER CONSIDERADAS MOEDAS?

Há um grande debate sobre se as criptomoedas podem ou não ser consideradas moedas. Em muitas teorias econômicas, postula-se que as moedas devam atender a três critérios básicos: ser "reserva de valor", "meio de troca" e "unidade de conta".

Muitos argumentam que, como quase ninguém precifica **nativamente** bens e serviços em criptomoedas, elas não cumprem a função de "unidade de conta". Até existem mercados virtuais onde os preços dos bens e serviços são exibidos em unidades de criptomoedas (bitcoin, por exemplo), mas sempre calculados em função de um preço base em moeda nacional (dólar americano, tipicamente), multiplicado pelo preço da criptomoeda nas corretoras naquele instante. Como o preço das criptomoedas é muito volátil, variando significativamente em questão de horas, não há como fazer os preços dos bens e serviços parecerem estáveis.

Não menos controverso é conceito de "reserva de valor": para muitos, as próprias moedas fiduciárias não provêem esta característica, dado que as políticas monetárias das maiorias dos governos almejam uma inflação de 2% ao ano (ou seja, perde 99% do seu valor em um século), como estímulo ao consumo (tornando melhor gastar o dinheiro do que guardá-lo). Se a moeda fiduciária fosse uma boa reserva de valor, não haveria necessidade de investimentos tais como "caderneta de poupança" e outros que buscam maiores retornos. Sob essa visão, o máximo que as moedas nacionais provêem é uma "ilusão" de preços aparentemente estáveis no curto prazo.

Os defensores das criptomoedas também citam o fato que elas oferecem recursos que as moedas fiduciárias não provêem (e aparentemente nem sequer vêm à mente dos economistas tradicionais como necessários ou desejáveis), como contabilização perfeita e auditabilidade universal, que permitem a qualquer participante independentemente verificar que nenhuma unidade monetária foi criada ou destruída fora das regras pré-estabelecidas do sistema.

Portanto, talvez o melhor caminho seja entender a palavra "moeda" dentro do termo "criptomoeda" apenas como uma analogia útil mas imperfeita, e reconhecer as semelhanças e diferenças entre as moedas e criptomoedas como inerentes a suas distintas naturezas.

criptomoeda de privacidade

❶ ("*privacy coin*", em inglês) criptomoeda em que os endereços de origem e destino, bem como os valores transacionados, não são acessíveis a nenhum outro participante



senão os diretamente envolvidos na transação.

📖 *A Monero é a mais conhecida criptomoeda de privacidade, e a maior em termos de capitalização de mercado.*

📖 *Uma das coisas mais incríveis da Monero é seu uso de criptografia avançada para permitir que as transações continuem sendo independentemente auditáveis mesmo sem ser possível saber os valores e endereços de uma transação.*

defi

❶ (contração de “*decentralized finance*”, em inglês, tipicamente estilizado “DeFi”; ou “finanças descentralizadas”, em Português) conjunto de serviços e produtos financeiros, como empréstimos, transferências, sistemas de pagamentos, seguros ou negociações de ativos que rodam em redes baseadas em *blockchains*. As soluções DeFi *em tese* não possuem instituições financeiras como intermediárias e podem ser realizadas diretamente entre as partes por meio de contratos inteligentes.

descentralização

❶ princípio genérico de distribuir o controle, a autoridade e a tomada de decisões da forma mais direta e igualitária possível por todos os participantes de uma rede ou sistema, sem a necessidade ou existência de uma única pessoa, entidade ou ponto central de coordenação ou autoridade.

DESCENTRALIZAÇÃO: MAIS UM IDEAL DO QUE UMA REALIDADE

A descentralização é uma das características mais almejadas das criptomoedas, mas ela é surpreendentemente difícil de atingir e até de definir.

Por exemplo, pode-se argumentar que a rede Ethereum é descentralizada porque existem milhares computadores espalhados por diversos países participando no processamento e repasse das transações.

Porém, alguns têm mais poderes do que outros: os “validadores” confirmam as transações e criam novas unidades monetárias, enquanto um participante normal, não. Como tornar-se validador custa caro (pelo menos 32 Ether, equivalente a algumas centenas de milhares de reais), há uma tendência à centralização favorecendo os mais ricos.

Outro exemplo: imagine um contrato inteligente em uma rede descentralizada, como o Ethereum, implementando um token. Como o contrato nada mais é que um programa de computador, o autor do contrato dita todas as regras do seu comportamento, agindo como centralizador, e seus usuários podem apenas segui-las.

Outra possibilidade seria uma criptomoeda descentralizada em quase todos os aspectos, mas que tem só três ou quatro desenvolvedores. Eles têm uma influência desproporcional em relação aos meros usuários, e isso pode ser considerado um tipo de centralização.

Quantificar a descentralização também é um desafio: uma métrica, por exemplo, poderia ser a razão entre a quantidade de usuários finais e a quantidade de validadores. Outro critério pode ser a distribuição geográfica. E outro ainda poderia não só a quantidade, mas a igualdade ou disparidade de poderes entre os vários participantes.

Uma busca no Google por "**quantifying decentralization**" revela diversos artigos acadêmicos propondo diferentes metodologias, deixando claro a vastidão e complexidade do assunto.

Por isso, o termo "descentralização" não deve ser entendido como algo binário, que ou se tem, ou não se tem; antes, é algo que se pode ter em maior ou menor grau, e em níveis ou aspectos diferentes – e que, na prática, tem sido mais um ideal do que uma realidade.

dex

❶ abreviatura de "decentralized exchange", mesmo que: ➤ corretora descentralizada.

distribuído

❶ diz-se de um sistema cujos participantes estão espalhados em diferentes pontos da internet ou localizações geográficas.

📖 *Um sistema ser "distribuído" não é a mesma coisa que "descentralizado". Há muitos sistemas distribuídos que são centralizados ou centralizantes.*

distributed ledger technology

❶ mesmo que: ➤ tecnologia de livro-razão distribuído.

DLT

❶ abreviatura de "Distributed Ledger Technology", veja: ➤ tecnologia de livro-razão distribuído;

dogecoin

❶ (símbolo "DOGE") criptomoeda originada em 2013 como uma brincadeira ou meme, incorporando a imagem do Shiba Inu do meme "Doge" da internet. Apesar de suas origens cômicas, acabou ganhando adoção suficiente para frequentemente figurar entre a lista das dez maiores criptomoedas por capitalização de mercado. Tornou-se conhecida pelo seu uso para gorjetas ou doações, por sua comunidade engajada, e por ter sido promovida até pelo Elon Musk, colocando-a como "a primeira, mais antiga e mais famosa das memecoins".

📖 *A adoção da Dogecoin foi facilitada por ser merge-mineable com a Litecoin e outras que usem o algoritmo Scrypt.*



DYOR

❶ abreviatura de “Do Your Own Research” (“faça sua própria pesquisa”), usado como ressalva de que não se deve necessariamente confiar unicamente nas opiniões sendo apresentadas, nem tomá-las como recomendação de investimento, e, ao invés, pesquisar outras fontes e formar sua própria opinião, assumindo responsabilidade total por ela.

ecossistema bitcoin

❶ a rede Bitcoin juntamente com os diversos serviços que a usam como base, tais como as corretoras, exploradores, carteiras, etc.

E2EE

❶ abreviatura de “end-to-end encryption”, *mesmo que:* • criptografia fim-a-fim;

EIP

❶ (sigla de “Ethereum Improvement Proposal”, ou “Proposta de Melhoria do Ethereum”) série de documentos técnicos detalhando minuciosamente propostas para novos recursos e melhorias no Ethereum ou em seu entorno, bem como seus prós e contras, para debate entre os desenvolvedores e servindo de guia para os que forem implementá-la. Algumas propostas não pegam tração, mas algumas são implementadas, resultando em uma nova versão da implementação de referência ou de algum dos programas/sistemas adjuntos. ❷ (juntamente com o número, p. ex., “EIP-1559”) um documento específico dentro dessa série.

endereço

❶ uma sequência de caracteres (letras e números) para os quais valores em criptomoedas podem ser enviados, vagamente análogo aos “números de contas” dos sistemas tradicionais. Contudo, na verdade os endereços são abreviaturas/ identificadores de programas de computador (chamados em certos contextos de “scripts”, e em outros de “contratos inteligentes”) que definem as regras ou condições para que aqueles fundos possam ser movidos.

📖 *Na maioria das criptomoedas, os endereços são calculados em função das chaves públicas e estas, por sua vez, em função das chaves privadas;*

endereço de queima

❶ endereço deliberadamente criado com uma chave privada desconhecida, tornando os fundos para ele enviados indefinidamente travados ou “queimados”. Alguns endereços de queima são propositalmente criados de forma a serem fáceis de reconhecer visualmente, incorporando palavras ou frases que fazem sentido quando lidas e/ou mencionam o nome do projeto a qual pertencem.

equity token

① ativos tradicionais de ações, que representam uma participação em determinadas empresas subjacentes, registrados em uma rede baseada em *blockchain*.

ETH

① Abreviatura de “Ether”, como unidade de conta. Apesar de tradicional e popular, essa abreviatura conflita com as regras do padrão ISO 4127.

ether

① (tipicamente pronunciado pelos brasileiros como “éter”, soa mais como “íter” quando falado pelos estrangeiros; símbolo: Ξ) unidade de conta da criptomoeda Ethereum. ② o preço de um ether relativo a alguma moeda nacional;

📖 *Você manda Ether e ele te paga em reais.*

📖 *O preço do ether despencou hoje.*

ethereum

① (tradicionalmente com inicial maiúscula) uma das mais populares criptomoedas do mundo, pioneira na introdução do conceito de “contratos inteligentes” e “dinheiro programável” que facilita a criação de tokens para finalidades específicas; ② o preço de uma unidade de Ethereum relativo a alguma moeda nacional;

📖 *Conta a lenda que o Vitalik Buterin criou o Ethereum porque os desenvolvedores do Bitcoin não queriam os problemas de segurança associados aos contratos inteligentes;*

📖 *O Ethereum caiu um pouco hoje. Ou melhor, quem caiu foi o preço do Ethereum, a rede em si continua de pé!*

ethereum virtual machine

① (frequentemente abreviado EVM): o “motor” ou “computador simulado”, capaz de computabilidade universal, que executa os contratos inteligentes na rede Ethereum.

📖 *Diversos outros projetos oferecem compatibilidade com a EVM, tais como Polygon, Cardano, Hyperledger Besu, etc.*

EUR

① abreviatura de Euro, a moeda comum da Europa, segundo o padrão ISO 4217.

EVM

① abreviatura de “Ethereum Virtual Machine”, veja [etherium virtual machine](#); ②

padrão técnico que especifica o funcionamento dos cartões de débito e crédito com chips (“smart cards”), sigla de “Europay, Visa, Mastercard”, as três empresas que originaram o padrão.

exchange

❶ no Brasil, usado em larga medida como sinônimo de “corretora”, embora o significado original seja “casa de câmbio”.

explorador

❶ tipo de site acessível pelo navegador em que exibe os dados dos *blockchains* de uma ou mais criptomoedas de forma analítica e detalhada para conferência manual, tipicamente permitindo pesquisar transações, blocos, endereços a partir de seus identificadores, mostrando seu conteúdos, datas, valores transferidos, scripts, contratos, etc.

fan token

❶ tipo de token de utilidade concebido para serem adquiridos ou colecionados por fãs de celebridades, torcedores de times esportivos, etc.

fiat

❶ (“faça-se”, em latim) alguma moeda nacional (real, dólar, etc.) que deve sua existência e valor a um decreto governamental.

fill or kill

❶ (“preencher ou matar”; frequentemente abreviado “FOK”) tipo de ordem de compra ou venda em uma corretora que ou é integralmente executada nas condições acordadas (a um preço específico, tipicamente), ou que é totalmente descartada, sem execução parcial, evitando deslize (“*slippage*”).

fork (criptomoedas)

❶ (“bifurcação” no sentido de “ruptura”, “cada um pro seu lado”): ato raro e frequentemente traumático, em geral resultante de uma dissidência irreconciliável entre sua comunidade de desenvolvedores, de separar uma criptomoeda em duas, com o histórico de transação até o ponto de ruptura compartilhado mas seguindo independente para cada uma a partir dali. O “fork” de uma criptomoeda implica em um “fork” do código fonte, daí a frequente confusão entre os diferentes significados do termo.

📖 *O fiasco do TheDAO causou o fork entre o Ethereum e o Ethereum Classic.*

📖 *O Bitcoin Cash é um fork do Bitcoin causado pela controvérsia ao redor das*

testemunhas segregadas e o Grande Debate do Tamanho do Bloco.

fork (desenvolvimento de software)

❶ (raramente traduzido para Português e quase sempre mantido em inglês, mas significa “bifurcação”): ato relativamente corriqueiro de pegar o código fonte de um programa ou sistema e usá-lo como base inicial ou parte de um novo projeto.

fungível

❶ substituível por outro do mesmo tipo ou classe sem perda valor ou funcionalidade; indistinguível em natureza ou qualidade, a ponto de qualquer um específico ser tão bom quanto qualquer outro.

📖 *Se não estiverem rasgadas, as cédulas são consideradas fungíveis: uma nota de cinquenta reais limpinha vale os mesmos cinquenta reais que uma cédula dobrada, amassada ou com um bigodinho desenhado na Efigie da República.*

📖 *Originalmente os bitcoins foram concebidos para serem fungíveis, viabilizando agirem como moeda; contudo, a reinterpretação deles como Ordinals tornam alguns satoshis mais desejáveis, valiosos, “coleccionáveis” – ou seja, infungíveis.*

gas

❶ unidade que mede o custo computacional necessário para executar transações ou contratos inteligentes, análogo à taxa de mineiro de outras criptomoedas. O preço do gas é pago aos validadores para incentivar o processamento das transações e a conservação de recursos, desincentivando spam.

gibi-

❶ (abreviatura: “Gi”) prefixo que significa 1.073.741.824 (2^{30}), usado quando há necessidade de se ser exato; por ser próximo de um bilhão, frequentemente usa-se “giga” ao invés, quando a diferença não importa muito.

📖 *A diferença entre um gibi e um giga é de uns 73 mega.*

giga-

❶ (abreviatura: “G”) prefixo que significa “bilhão” (10^9 ou 1.000.000.000).

📖 *O tamanho do blockchain do bitcoin, sem índices, já passa dos 487 gigabytes.*

📖 *O preço do gas no Ethereum normalmente é medido em gwei.*

Gwei

❶ abreviatura de “gigawei”, ou um bilhão de wei, a unidade corriqueira para medir

preços de gas no Ethereum.

halving

❶ (pronuncia-se algo como "révin", embora muitos brasileiros pronunciem "rólvin") queda pela metade na recompensa de mineração que ocorre periodicamente em certas redes de criptomoedas. Nas redes Bitcoin e Bitcoin Cash, o halving acontece a cada 210 mil blocos, ou cerca de 4 anos. No Litecoin, ocorre a cada 840 mil blocos, ou aproximadamente a cada 4 anos. As sucessivas meações fazem com que a quantidade máxima de unidades monetárias atinja um valor máximo pré-estabelecido (na rede Bitcoin, ligeiramente menos que 21 milhões).

📖 *A cada halving a oferta de novas unidades da moeda cai pela metade, o que, mantendo-se a demanda, tende a eventualmente dobrar o preço.*

hash

❶ (sem equivalente em Português; pronuncia-se "résh") em Ciência da Computação, um dentre vários procedimentos de cálculo que transformam dados de qualquer tamanho em um número de um certo tamanho máximo fixo (no mundo das criptomoedas, tradicionalmente escritos como 64 dígitos hexadecimais, o que equivale a 78 dígitos decimais ou 256 dígitos binários). Em conjunto com o fato de terem uma distribuição uniforme, viabiliza serem usados como identificadores únicos e verificadores anti-adulteração. ❷ o resultado desse cálculo; ❸ o resultado desse cálculo para uma transação ou bloco específico. ❹ no contexto de mineração, quantidade de vezes que esse cálculo foi feito; ❺ sinônimo informal (embora tecnicamente incorreto) para "hashes por segundo".

📖 *Um hash que todo mundo usa sem se dar conta são dos dígitos verificadores do CPF.*

📖 *O identificador da transação nada mais é que o hash do seu conteúdo.*

📖 *Se A e B têm o mesmo hash, significa que eles são idênticos bit a bit – o que pode ou não significar que eles são visualmente idênticos, a depender do tipo exato do arquivo.*

📖 *Um subproduto do processo de mineração é que os hashes dos blocos, quando escritos na forma tradicional de 64 dígitos em hexadecimais, começam sempre com pelo menos oito zeros.*

📖 *O custo do bloco gênese do Bitcoin foi de uns 4,3 gigahashes.*

📖 *Antigamente, uma mineradora capaz de atingir 13 terahashes custava uma*

pequena fortuna.

hashes por segundo

① unidade de medida de velocidade de mineração, no contexto de sistemas baseados em prova de trabalho.

📖 *Minha nova mineradora faz 135 terahashes por segundo!*

📖 *Estima-se que a velocidade de mineração da rede bitcoin global exceda os 400 milhões de terahashes.*

hexadecimal

① sistema de numeração em que, além dos dígitos 0 a 9, há ainda mais seis, tradicionalmente grafados com as letras de A a F, representando os valores de 10 a 15. Por ser mais próximo do sistema binário (que é como o processamento dos dados é realmente realizado nas entranhas dos computadores), encurta a grafia e simplifica os cálculos em muitos casos, tornando-se preferido pelos desenvolvedores e cientistas da computação. Em certos contextos, vêm precedido por 0x para explicitar que se trata de um número em hexadecimal.

📖 *No Ethereum, tanto os endereços, quanto identificadores de transações e blocos são tradicionalmente grafados em hexadecimal.*

hodl

① (erro de digitação da palavra em inglês “hold”, que significa “segurar”, que virou meme): guardar uma certa quantidade de criptomoedas por longo prazo (anos, tipicamente), na esperança que aumente de valor, independente das flutuações de curto prazo.

📖 *O termo “HODL” surgiu de um erro de digitação que um usuário do forum BitcoinTalk chamado “GameKyuubi” cometeu ao explicar que ele pretendia guardar suas criptomoedas por um longo prazo porque ele se considerava um “trader ruim”. Posteriormente inventaram um significado de “Hold On for Dear Life” (“segure por sua própria vida”), mas não era esse o significado original.*

hodler

① detentor de criptomoedas que pratica, ou defende a prática, de guardar criptomoedas por longos períodos, ou, no extremo, “jamais vender”. *Veja também:* [hodl](#).

hot storage

① *mesmo que:* ➤ [armazenamento quente](#);

hot wallet

① *mesmo que:* ➤ [armazenamento quente](#);

kibi-

① (abreviatura: “Ki”) prefixo que significa 1024 (2^{10}), usado quando há necessidade de se ser exato; por ser próximo de mil, frequentemente usa-se “kilo” ao invés, quando a diferença não importa muito.

📖 *A diferença entre um kibibyte e um kilobyte são só 24 bytes.*

kilo-

① (abreviatura: “K” maiúsculo) prefixo que significa “mil” (10^{+3} ou 1.000).

📖 *Os Inscriptions permitem colocar dados com vários kilobytes direto no blockchain do Bitcoin, muito mais que as transações Null Data, que só permitam meros 80 bytes.*

ICO

① abreviatura de “Initial Coin Offering”, vide ➤ [initial coin offering](#).

initial coin offering

① lançamento de um novo token ou criptomoeda ao público, às vezes sob preços ou condições especiais, como uma forma de arrecadar fundos para o desenvolvimento ou expansão do projeto, em analogia aos IPOs (Initial Public Offerings) no mercado de ações, mas no âmbito de uma rede criptomoedas e corretoras parceiras, porém sem direitos de participação ou governança, e fora da supervisão regulatória.

inscrições

① método criado em dezembro de 2022 para armazenamento de arquivos relativamente grandes (centenas de kilobytes) dentro do próprio *blockchain* do Bitcoin, cuja propriedade pode ser transferida e rastreada tal como os próprios bitcoins, criando uma espécie de token infungível. Os arquivos podem ser de qualquer tipo: textos, PDFs, imagens, vídeos, programas de computador, etc.

inscriptions

① *mesmo que:* ➤ [inscrições](#).

inverno

❶ *bear market* (momento de desânimo, pessimismo e preços baixos no mercado) particularmente longo, persistindo por vários meses ou até anos.

lambo

❶ (contração de "Lamborghini", marca italiana de carros esportivos de luxo) expectativa ou desejo de um aumento tão grande no valor de uma criptomoeda que permitiria ao detentor ficar tão rico a ponto de poder comprar um Lamborghini. Usado tanto de maneira séria pelos entusiastas, quanto de maneira irônica por críticos.

lightning network

❶ *mesmo que:* ➤ rede relâmpago.

litecoin

❶ (tradicionalmente com inicial maiúscula) clone do bitcoin criado em 2011 por Charlie Lee, oferecendo tempos entre blocos de 2,5 minutos (quatro vezes mais rápidos que o bitcoin) e uma função de trabalho computacionalmente mais pesada que a do bitcoin, que se acreditava que impediria a mineração usando ASICs (e, portanto, só seria viável em computadores tradicionais, evitando a centralização da mineração, daí o termo "lite") – mas, que contudo, posteriormente provou-se irreal. ❷ (tradicionalmente com inicial minúscula; símbolo: ₪) a unidade de conta desta criptomoeda; ❸ o preço de uma unidade de litecoin relativo a alguma moeda nacional; ❹ sinônimo informal para "rede Litecoin"; ❺ o programa de computador que implementa todo esse sistema;

📖 *Um dos slogans do Litecoin era "se o Bitcoin é o ouro digital, Litecoin é a prata".*

KYC

❶ (sigla em Inglês de "know your customer", ou, em Português, "conheça seu cliente") medidas que os governos obrigam as corretoras e agentes do mercado financeiro tradicional a adotarem para identificar as pessoas físicas responsáveis pelas transações financeiras, para que possam ser responsabilizadas em caso de ilícitos.

livro de ofertas

❶ parte essencial de uma corretora, disponibilizado através de um site, aplicativo ou API, onde os vendedores e compradores cadastram suas ofertas, mencionando preço unitário e quantidade de um ativo que desejam vender ou comprar, concretizando o negócio quando o preço de compra e de venda coincidem.

mainnet

❶ ("rede principal", em inglês): a rede principal de uma criptomoeda, cujas unidades monetárias são aceitas pelas corretoras e têm valor de revenda. *Contraste com:* ➤ ..

testnet.

mão de alface

① (gíria) indivíduo propenso a vender seus ativos em pânico, sob preços ou condições desfavoráveis, perdendo dinheiro ou oportunidades. *Veja também:* • [alface](#).

market cap

① contração de “market capitalization”: • [capitalização de mercado](#).

market capitalization

① mesmo que: • [capitalização de mercado](#).

maxi

① contração de: • [maximalista](#).

📖 “Depois de se queimar tanto com as alts, ele acabou se tornando maxi.”

📖 “Aquela conferência só dá maxi.”

maximalista

① diz-se de alguém que defende vigorosamente a posição de que o Bitcoin é a única criptomoeda que vale a pena existir.

📖 “Esse Michael Saylor é um tremendo maximalista, não?”

mebi-

① (abreviatura: “Mi”) prefixo que significa 1.048.576 (2^{20}), usado quando há necessidade de se ser exato; por ser próximo de um milhão, frequentemente usa-se “mega” ao invés, especialmente quando a diferença não importa muito.

📖 *A diferença entre um mebi e um mega é de pouco menos de 48 kibi.*

mecanismo de consenso

① estratégia ou critérios adotados por uma criptomoeda e seu respectivo *blockchain* para determinar quais candidatos a novos blocos, dentre múltiplos candidatos igualmente aceitáveis, devem ser efetivamente aceitos e oficializados.

MECANISMOS DE CONSENSO SÃO CRITÉRIOS DE DESEMPATE

Os chamados “mecanismo de consenso” dos **blockchains** talvez seriam melhor descritos como “critérios de desempate”: quando dois mineradores ou validadores encontram, mais ou menos ao mesmo tempo, duas ou mais soluções diferentes igualmente válidas para fechar o próximo bloco, esse “critério de desempate” é usado para decidir qual das soluções

se tornará a oficial, e todas as outras são simplesmente descartadas. Não há negociação, nem análise de mérito ou qualidade: o critério de desempate é um cálculo matemático relativamente simples que dá um resultado claro, sem ambiguidade e auditável.

Essa clareza faz com que todos os participantes de uma rede descentralizada eventualmente convirjam para uma mesmo histórico das transações/eventos registrados. Contudo, existem vários tipos de critérios de desempate, sendo a "prova de trabalho" e a "prova de participação" os mais famosos, e há verbetes neste glossário descrito cada um deles. Há ainda alguns critérios menos conhecidos, como "prova de queima", "prova de autoridade", "prova de espaço (de armazenamento)" e talvez vários outros.

Atente também para o fato que existem alguns "prova de" que não são mecanismos de consenso. Por exemplo, a "prova de desenvolvedor" tenta identificar quem são os reais desenvolvedores de uma criptomoeda ou token, para evitar que um projeto seja "sequestrado" por fraudadores; a "prova de individualidade" ("proof of personhood"), que tenta determinar se há um ser humano de fato envolvido em um processo, para evitar ataques automatizados por "robôs"; e as "provas de conhecimento zero" são um conjunto de técnicas da disciplina de criptografia usadas em diversas criptomoedas para melhorar a privacidade dos dados nas transações.

A lição a ser aprendida é que, no mundo dos blockchains, o significado do termo "consenso", embora vagamente semelhante, é bem distinto do seu uso coloquial como "convergência de opiniões oriunda de debate, negociação e talvez até concessões": na verdade, trata-se de um critério para desempatar candidatos a novos blocos quando dois são propostos ao mesmo tempo.

mega-

❶ (abreviatura: "M" maiúsculo) prefixo que significa "um milhão" (10^6 ou 1.000.000).

📖 *O tamanho máximo de um bloco na rede bitcoin é 4 megabytes.*

memecoin

❶ criptomoeda criada a título de piada ou brincadeira, por vezes baseada em memes ou fenômenos culturais da internet, sem intenção de se tornar algo sério. Mesmo assim, algumas atingem adoção e capitalização de mercado consideráveis.

📖 *Doge é a memecoin favorita do Elon Musk.*

merged mining


❶ ("mineração combinada", em inglês) processo que permite minerar duas ou mais criptomoedas diferentes ao mesmo tempo sem custos adicionais, desde que tenham sido explicitamente projetadas para isso (compartilhem o mesmo algoritmo de prova de trabalho, entre outros detalhes técnicos).



📖 Seguindo uma sugestão do próprio Satoshi Nakamoto, a Namecoin foi a pioneira no uso de merged mining, podendo ser minerada simultaneamente com bitcoin.

📖 Dogecoin e Litecoin podem ser mineradas simultaneamente via merged mining.

Merkle root

mesmo que  raiz de Merkle.

micro-

❶ (abreviatura: “μ” ou “u”) prefixo que significa “um milionésimo” (10^{-6} ou 0,000001).

📖 Tentaram emplacar o termo “bits” como sinônimo de “microbitcoin”, mas não pegou.

mili-

❶ (abreviatura: “m” minúsculo) prefixo que significa “um milésimo” (10^{-3} ou 0,001).

📖 Um milibitcoin parece pouco, mas já são mais de cem reais!

mineiro

mesmo que  minerador.

minerador


❶ membro de uma rede de criptomoeda baseada no conceito de “prova de trabalho”, responsável por receber as transações dos usuários, auditá-las e/ou executar seus contratos inteligentes, agrupá-las em blocos e publicá-los, e gerar novas unidades monetárias para serem postas em circulação, recebendo-as como recompensa pelo serviço prestado à rede; ❷ o computador que efetivamente realiza essas operações (normalmente no feminino, “mineradora”, contração de “máquina mineradora”). ❸ as pessoas físicas ou jurídicas que controlam e operam esses computadores.

📖 Os mineradores pagam suas contas de luz vendendo parte das novas unidades monetárias que produzem nas corretoras.


📖 Coletivamente, mineradores são a espinha dorsal do Bitcoin. Talvez nem seja um grande exagero dizer que eles são a rede Bitcoin.

moeda digital

❶ qualquer forma de dinheiro ou representação de valor que existe na forma de informações dentro de algum computador, podendo ser moeda virtual, eletrônica, ou criptomoeda.


 *Pode-se argumentar que o Real Brasileiro já é uma moeda digital, pois a maior parte do volume financeiro passa pelos computadores dos bancos e cada vez menos se usa papel-moeda.*

moeda virtual


 de acordo com o Banco Central Europeu (2012), um tipo de moeda digital não regulamentada, que: é emitida e geralmente controlada por seus desenvolvedores; é usada e aceita entre membros de uma comunidade virtual específica; em geral, não é baseada em *blockchains*.


 *Jogos como World of Warcraft, League of Legends, FIFA, Roblox têm suas próprias moedas virtuais.*

moeda eletrônica

 definida pela Lei 12.865/2013 como “recursos armazenados em dispositivo ou sistema eletrônico que permitem ao usuário final efetuar transação de pagamento”, posteriormente clarificado por comunicados nº 25.306/14 e 31.379/17 do Banco Central do Brasil como excluindo criptomoedas/criptoativos.

monero

 (“moeda”, em Esperanto; símbolo “XMR”) criptomoeda lançada em 2014 com foco em irrastreabilidade das transações, tida como a maior e mais famosa das “*privacy coins*”, que usa técnicas avançadas de criptografia para que seu histórico de transações não permita a observadores externos identificar os valores e endereços de origem ou destino, mas ao mesmo tempo preservando a auditabilidade universal.

 *Os proponentes da Monero argumentam que só pode haver fungibilidade se houver irrastreabilidade: se for possível saber o endereço de origem dos fundos, é sempre possível criar listas de bloqueio, criando uma divisão entre “dinheiro bom” e “dinheiro ruim”.*

nano-

 (abreviatura: “n” minúsculo) prefixo que significa “um bilionésimo” (10^{-9} ou 0,000000001).

 *Um gigawei (Gwei) é um nanoether.*

não-permissionado

 diz-se de uma rede baseada em *blockchains* ou DLTs em que as barreiras de entrada são tão baixas que podem ser consideradas universalmente abertas ao público em geral.

📖 *As redes de criptomoedas como Bitcoin, Ethereum, etc, são consideradas não-permissionadas.*

NFT

❶ abreviatura de “Non-Fungible Token”, vide [token infungível](#);

nó (redes de criptomoedas)

❶ um programa de computador atuando como participante ativo de uma rede de criptomoedas, recebendo blocos e transações dos usuários ou nós vizinhos, auditando-os e, se validados, repassando-os aos demais vizinhos. ❷ o computador onde esse programa está sendo executado; ❸ a pessoa física que opera e mantém esse computador;

nó (teoria dos grafos)

❶ o ponto onde uma ou mais arestas (linhas) se encontram, normalmente desenhado como uma bolinha.

nocoiner

❶ indivíduo que não possui, ou professa não possuir, criptomoedas.

node

❶ *mesmo que:* [nó](#).

oráculo

❶ sistema ou serviço que traz dados de fora de um *blockchain* (por exemplo, de um site ou API tradicional) para dentro dele, de forma que possa ser utilizado pelos contratos inteligentes sem ferir as necessidades de determinismo e reprodutibilidade, embora possivelmente em detrimento da descentralização.

order book

❶ *mesmo que:* [livro de ofertas](#).

ordem a mercado

❶ em corretoras, uma oferta de compra ou venda de uma certa quantidade de um ativo ao preço atual, que é executada instantaneamente, retirando dos livro as ofertas correspondentes das contrapartes.

ordem a limite

❶ em corretoras, uma oferta de compra ou venda a um preço específico mais alto ou mais baixo que o preço atual. Por diferir do preço atual, ela não é executada imediatamente; ao invés, é cadastrada no livro de ofertas, ficando visível para os

demais participantes, só será executada quando o preço atual atingir o preço de mercado.

ordem de parada

❶ (em inglês, “*stop-loss order*”, “*stop order*” ou apenas “*stop*”) em corretoras, uma ordem “invisível” (que não aparece no livro de ofertas) que se converte em uma ordem limite ou a mercado quando o preço cai abaixo de um patamar pré-determinado. Tipicamente usado para minimizar perdas em caso de quedas bruscas no preço.

ordinais

❶ na rede Bitcoin, interpretação da ordem de criação dos satoshis que lhes confere significados e valores especiais de acordo com os vários ciclos do bitcoin (meações, reajustes de dificuldade, etc.)

ordinals

❶ *mesmo que:* ordinais.

OTC

❶ (sigla em inglês para “Over the Counter”; em português, “pelo balcão”) serviço de compra e venda de criptoativos em grandes volumes oferecidos por algumas corretoras, apartado dos livros de ofertas.

OTP

❶ em cybersegurança, sigla de “One-Time Password”; veja: senha descartável. ❷ em criptografia, abreviatura de “One-Time Pad”, um ideal teórico de cifragem que é total e perfeitamente aleatório e que só é usado uma única vez, sendo descartado após o uso.

P2P

❶ (abreviatura de “peer to peer”, significando “entre pares (indivíduos)”); por vezes traduzido como “ponto a ponto”, devido ao fato do termo “par” em Português não evocar a imagem de “indivíduo”) ❷ algum tipo de transação feita diretamente entre os indivíduos ou participantes de um sistema, sem a necessidade de um intermediário; ❸ mercado informal ou semi-formal de pessoas físicas que compram ou vendem criptomoedas diretamente entre si, sem passar por corretoras, empresas ou pessoas jurídicas.

Comprar ou vender Bitcoin no P2P só é viável para valores relativamente pequenos.

paper wallet

❶ *mesmo que:* ➤ [carteira de papel](#);

permissionado

❶ diz-se de uma rede baseada em blockchains em que o acesso ou participação é restrita, sujeita à aprovação de um dono ou centralizador, ou cujas barreiras de entrada são elevadas.

📖 *O Real Digital roda em um blockchain permissionado, só instituições financeiras aprovadas pelo BACEN podem participar.*

PoB

❶ abreviatura de "Proof of Burn", vide ➤ [prova de queima](#);

PoS

❶ abreviatura de "Proof of Stake", vide ➤ [prova de participação](#);

PoW

❶ abreviatura de "Proof of Work", vide ➤ [prova de trabalho](#);

proof of burn

❶ *mesmo que:* ➤ [prova de queima](#);

proof of stake

❶ *mesmo que:* ➤ [prova de participação](#);

proof of work

❶ *mesmo que:* ➤ [prova de trabalho](#);

prova de participação

❶ (em inglês, "Proof-of-Stake", abreviado "PoS") metodologia de consenso em que o validador tende a produzir novas unidades monetárias de forma aproximadamente proporcional à quantidade de fundos colocados em caução. Por envolver provas criptográficas, pode ser auditada independentemente por qualquer participante, viabilizando arquiteturas descentralizadas. *Contraste com:* ➤ [prova de trabalho](#).

📖 *O Ethereum reduziu seu consumo de energia em 99% após trocar de prova de trabalho para prova de participação.*

prova de queima

❶ (em inglês, "Proof-of-Burn", abreviado "PoB") metodologia de consenso

descentralizada em que os participantes tornam inutilizáveis (“queimam”) suas próprias criptomoedas enviando-as para um endereço do qual não podem ser recuperadas. A probabilidade de um participante ter suas propostas de novos blocos incorporadas é aproximadamente proporcional à quantidade de moedas que ele queimou. Como os endereços de queima são públicos, é possível auditar quando e quantas moedas foram queimadas.

📖 *Um dos primeiros sistemas a utilizar prova de queima foi o protocolo Counterparty.*

prova de trabalho

① (em inglês, “Proof of Work”, abreviado “PoW”; também conhecido como “consenso de Nakamoto”) metodologia de consenso em que a capacidade de um minerador criar novas unidades monetárias é aproximadamente proporcional à quantidade de trabalho computacional que ele realiza (que, por sua vez, consome recursos escassos na vida real, como eletricidade). Em caso de propostas simultâneas e igualmente válidas para o próximo bloco, a quantidade total de trabalho realizado até então é usada como critério de desempate. Este processo, que envolve provas criptográficas verificáveis por qualquer participante, facilita arquiteturas que dispensam coordenadores ou árbitros centralizados. *Contraste com:* ➤ prova de participação.

📖 *Entre as principais criptomoedas baseadas em prova de trabalho pode-se citar: Bitcoin e seus derivados (Bitcoin Cash, Litecoin, Namecoin, Dogecoin, Dash, ZCash), Monero, etc.*

provas de conhecimento zero

① (em inglês, “zero-knowledge proofs”, abreviado “ZKPs”) métodos estudados pela disciplina de criptografia em que um participante (chamado “proponente”) demonstra para outro participante (chamado “verificador”) que conhece ou detém uma determinada informação, ou que a informação é verdadeira, sem revelar nada que possa servir de pista para que o verificador descubra a informação em si. Várias criptomoedas e sistemas de finanças descentralizadas (DeFi) adotam ZKPs para promover maior privacidade nas transações, protegendo a identidade dos participantes, os endereços de envio e recebimento utilizados e/ou os valores transacionados.

pump and dump

① (em Português, “inflar e despejar”) ato de inflar artificialmente o preço de um ativo, comprando-o maciçamente nas corretoras (“pump”) e disseminando informações falsas ou enganosas para atrair outros investidores, para logo em seguida vendê-lo rapidamente e em grandes quantidades (“dump”), causando uma queda abrupta nos preços. Em muitos contextos e jurisdições, essa atividade é considerada manipulação




de mercado e, portanto, ilegal.

raiz de Merkle

❶ (“Merkle root”, em inglês, em homenagem ao seu inventor, o cientista da computação Ralph Merkle) resultado do processo de se calcular o hash de uma lista de itens quaisquer (tipicamente transações) agrupando-os em pares, resultando em uma lista com metade da quantidade original de itens, e repetindo o processo até chegar a uma lista de um elemento só, sendo esse elemento o resultado final. ❷ campo do cabeçalho dos blocos da rede Bitcoin (e de várias outras criptomoedas) contendo o valor da raiz de Merkle calculado a partir da lista de todas as transações contidas naquele bloco.

rede bitcoin

❶ o conjunto de todos os nós (computadores) participantes do processo de construção coletiva do blockchain do Bitcoin. Essa definição estrita exclui as corretoras, exploradores, etc. *Contraste com:*  [ecossistema bitcoin](#).

rede relâmpago


❶ (em inglês, “Lightning Network” ou “LN”) rede que cria canais de pagamento privados entre os participantes, lastreados em trava de recursos em arranjos semelhantes a “contratos inteligentes”, e permitindo roteamento entre diferentes canais, resultando em baixíssimas taxas de transação que viabilizam micropagamentos e finalização quase instantânea (poucos segundos). Pode funcionar com várias criptomoedas, e tanto a rede Bitcoin quanto a Litecoin têm suas próprias redes relâmpago. Por ser tecnicamente uma rede adjunta mas separada, é considerada uma “solução de segunda camada” (a “primeira camada” sendo a própria criptomoeda onde se baseia) e deu origem a todo um outro ecossistema de soluções de pagamento.

sat

❶ abreviatura de “satoshi”, a unidade de conta.

satoshi

❶ (em minúsculas, abreviado “sat”) unidade de conta equivalente a 0,00000001 (10^{-8}) bitcoin, que é a menor quantidade possível de ser representada. ❷ (em maiúsculas) prenome do inventor do Bitcoin, Satoshi Nakamoto.

 *As taxas de mineiro da rede bitcoin são tipicamente medidas em satoshis por byte.*

Satoshi Nakamoto

❶ o pseudônimo do inventor do Bitcoin, cuja identidade real até hoje permanece desconhecida.

sandbox

① ambiente apartado, tipicamente temporário ou descartável, que simula com razoável realismo, mas em menor escala e de forma controlada, as características de um sistema maior e mais complexo, para fins de ensaio ou testes, de sorte que erros, imprevistos ou desastres não tenham consequências sérias.

sandbox regulatório

① ambiente criado por entidades regulatórias, como a Comissão de Valores Mobiliários, onde certos requisitos regulatórios são dispensados, para que novos produtos ou serviços considerados inovadores sejam testados antes de irem a público, ajudando também a identificar necessidades de alterar regulações já existentes, ou criar novas, para prover regulação adequada às novidades introduzidas.

script

① uma linguagem (deliberadamente restrita para não ser capaz de computabilidade universal) utilizada na rede Bitcoin e derivadas para especificar condições que testam se uma transferência de criptomoedas pode ser autorizada ou não. ② Um teste de autorização específico expresso nessa linguagem.

📖 *Há quem diga que os scripts do Bitcoin são “contratos ‘burros’”, antes de virarem “inteligentes” (universalmente programáveis) como no Ethereum.*

📖 *A linguagem de script do Bitcoin é baseada em Notação Polonesa Reversa, semelhante às antigas calculadoras HP-12C populares nos anos 80.*

📖 *No Bitcoin, as chaves privadas dão origem às chaves públicas, que tipicamente vão inclusas nos scripts, que, por sua vez, dão origem aos endereços.*

security token

① representação de um valor mobiliário dentro de uma criptomoeda ou plataforma baseada em blockchain, para que adquira as características inerentes dela, ao mesmo tempo preservando a aderência regulatória associada aos valores mobiliários.

segregated witness

① *mesmo que:* ➤ testemunhas segregadas.

segwit

① abreviatura de “segregated witness”, veja: ➤ testemunhas segregadas.

semente

① conjunto de 12 a 24 palavras que as carteiras usam para criar uma série de chaves



privadas, e, por conseguinte, endereços de recebimento. ② de forma mais geral, na disciplina de criptografia, qualquer dado (normalmente sigiloso) que dá origem a uma sequência de outras informações, como senhas descartáveis, chaves privadas, ou números aleatórios.

📖 *É imperativo que a semente não seja perdida nem caia em mãos erradas, sob o risco de se perder quaisquer criptomoedas depositadas nos endereços correspondentes.*

📖 *Aumento da privacidade nas transações é um dos benefícios de se ter seus fundos espalhados em múltiplos endereços.*

senha descartável

① (em inglês, “OTP”, sigla de “One-Time Password”) Uma senha que é mudada após cada uso, ou próximo disso. Normalmente o usuário tem um aplicativo no seu celular que calcula a nova senha (tipicamente um número de 6 dígitos) e que muda a cada 30 segundos, a partir de uma semente previamente cadastrada.

📖 *Praticamente toda corretora hoje em dia adicionou OTP ao formulário de login.*

📖 *Na maioria dos sites e aplicativos, a senha normal é normalmente o “primeiro fator de autenticação” e a senha descartável (OTP) normalmente é o “segundo fator de autenticação” (2FA).*

SHA256

① (abreviatura de “Secure Hash Algorithm”) algoritmo de *hash* usado na prova de trabalho do Bitcoin e várias outras criptomoedas, como Bitcoin Cash, Namecoin, etc. Também é largamente utilizado em diversas outras áreas da Ciência da Computação como verificador de integridade ou como parte de esquemas de assinaturas digitais. O número 256 se refere ao fato de seu resultado ter 256 bits de comprimento (equivalente a 78 dígitos decimais). *Veja também:* ➤ [hash..](#)

shill

① pessoa que promove um produto ou serviço de uma pessoa, empresa ou organização, sem revelar ou admitir explicitamente que tem um relacionamento próximo com aquela entidade.

simple payment verification

① *mesmo que:* ➤ [verificação de pagamento simplificada;](#)

simplified payment verification

① *mesmo que:* ➤ [verificação de pagamento simplificada;](#)

slippage

❶ (“deslize”, em inglês) diferença entre o preço de compra ou venda originalmente calculado e o realmente executado, oriundo do fato que outras negociações podem ter acontecido entre o momento do cálculo inicial e a efetiva execução da compra/venda, ou por falta de liquidez suficiente no mercado. *Contraste com:* ➤ fill or kill.

smart contract

❶ *mesmo que:* ➤ contrato inteligente.

solidity

❶ linguagem de programação de alto nível para escrever contratos inteligentes em redes baseadas na máquina virtual Ethereum (EVM).

spam

❶ transações desnecessárias ou sem sentido que congestionam as redes de criptomoedas, causando demora nas confirmações e/ou inflando as taxas. As taxas existem exatamente para desincentivar esse comportamento, tornando o envio de spam mais caro do que o uso legítimo e moderado.

SPV

❶ *mesmo que:* ➤ verificação de pagamento simplificada;

stablecoin

❶ criptomoeda que embute mecanismos para manter seu valor estável em relação a algum ativo ou grupo de ativos, normalmente uma moeda nacional estável ou uma cesta de moedas. Entre esses mecanismos, pode se citar: o respaldo direto por reservas do ativo de referência, algoritmos que ajustam a oferta da criptomoeda com base na demanda, ou contratos inteligentes que funcionam como sistema de caução.

📖 *O Tether (USDT) é, sem dúvida, a mais amplamente utilizada das stablecoins.*

taproot

❶ nome genérico de uma grande atualização no Bitcoin que entrou no ar em novembro de 2021 e introduziu um novo sistema de assinaturas digitais chamado Assinaturas de Schnorr, um novo formato de endereços chamado Bech32m que corrige uma deficiência no Bech32, e um novo sistema de scripting mais flexível que viabiliza “mini contratos inteligentes”.

taxa de mineiro

❶ valor escolhido e adicionado pelo originador de uma transação, em adição ao valor principal sendo transferido, para ser coletado pelos mineiros ou validadores,



incentivando-os a priorizar a transação e servindo também como desincentivo a spam.

📖 *Uma das funções das carteiras de criptomoedas é ajudar o usuário a selecionar o valor ideal da taxa para que a transação seja processada o mais rápido possível, ao mesmo tempo sem pagar mais que o estritamente necessário.*

tebi-

① (abreviatura: “Ti”) prefixo que significa 1.099.511.627.776 (2^{40}), usado quando há necessidade de se ser exato; por ser próximo de um trilhão, frequentemente usa-se “tera” ao invés, quando a diferença não importa muito.

📖 *A diferença entre um tebi e um tera é de quase 100 giga.*

tecnologia de livro-razão distribuído

① (“*distributed ledger technology*” em inglês, frequentemente abreviado “DLT”) termo cunhado após a criação do Bitcoin e seu respectivo *blockchain*, para designar uma ampla gama de abordagens ou plataformas de registro/notarização de transações que podem adotar uma ou algumas das características normalmente associados aos *blockchains*, como descentralização, contabilização perfeita, auditabilidade externa independente, código aberto, equipotência dos participantes.

📖 *Os proponentes do termo “DLT” tentam posicioná-lo como se blockchains fossem apenas um caso particular de DLTs em geral e que existem muitas outras abordagens parecidas, mas diferentes, dos blockchains, que podem ser mais adequadas a casos ou setores específicos.*

tera-

① (abreviatura: “T” maiúsculo) prefixo que significa “trilhão” (10^{12} ou 1.000.000.000.000).

📖 *O tamanho do blockchain do Ethereum nos nós de arquivamento já passa dos 14 terabytes.*

📖 *Estima-se que o consumo global de energia elétrica da rede bitcoin seja de pelo menos 68 terawatts-hora por ano.*


📖 *Uma boa mineradora faz pelo menos 100 terahashes por segundo.*


testnet

① (“rede de teste”, em inglês): uma rede de criptomoedas “*sandbox*” usada para seus desenvolvedores testarem as novas versões dos programas que implementam a rede e ensaiarem os procedimentos de atualização, identificando e corrigindo problemas,



antes de serem postos em prática na rede principal. *Contraste com:*  [mainnet](#).

 Quando rodando em modo *testnet*, vários parâmetros são mudados para torná-lo incompatível com a rede principal, para que não haja risco de se misturarem.


 A encarnação atual da *testnet* da rede Bitcoin, chamada *testnet3*, tem uma reputação de ser errática e frustrante de usar. Por isso, criaram a *signet*.

testemunha

❶ na disciplina de criptografia, algum dado que sirva como prova de que algum cálculo específico foi feito, tipicamente uma assinatura digital.

testemunhas segregadas

❶ (“*segregated witness*”, em inglês, por vezes abreviado “*segwit*”) nome genérico de uma grande atualização que entrou no ar na rede Bitcoin em 2017 que introduziu alterações profundas no formato das transações e blocos, onde as testemunhas (assinaturas digitais) ficam em uma área à parte (segregadas) e introduzindo um novo formato de endereços chamado *Bech32*. ❷ a seção onde esses dados se localizam dentro de uma transação.

 A controvérsia ao redor das *testemunhas segregadas* foi tão grande que causou um racha na comunidade e levou os dissidentes à criação de uma outra criptomoeda chamada *Bitcoin Cash*.

tether

❶ (abreviatura: “*USDT*”) a maior e mais famosa *stablecoin*, que se propõe a espelhar o preço do dólar americano. É considerada a espinha dorsal do mercado formado pelas corretoras de criptomoedas.

the merge

❶ (“*A Fusão*”, em inglês) evento na rede Ethereum, que vinha sido preparado há anos e finalmente ocorreu em setembro de 2022, onde o mecanismo de consenso da rede foi trocado de “*prova de trabalho*” para “*prova de participação*”, tida como talvez a mais radical guinada de direção jamais levada a cabo por uma criptomoeda até então.

token

❶ (sem equivalente em Português) a representação de algum bem, valor ou direito, comumente criada como contrato inteligente ou submoeda dentro de uma outra criptomoeda maior, ou, às vezes, como uma criptomoeda independente; ❷ a representação abstrata de um valor, bem, ou direito.



token de pagamento

❶ tipo de *token* cujo propósito principal esperado é a realização de pagamentos no dia a dia. Às vezes o termo é usado com a conotação de que o token existe em uma rede baseada em blockchains, mas às vezes também é usado sem essa conotação – pode ser necessário avaliar o contexto para inferir o significado exato.

📖 *Há quem encare as criptomoedas como um tipo de token de pagamento.*

📖 *O saldo em uma corretora ou no banco pode ser encarado como um tipo de token de pagamento representando a dívida que a instituição tem com o correntista.*

token de utilidade

❶ tipo de token que confere ao seu detentor benefícios úteis junto à instituição emitente, como descontos, acessos exclusivos a locais, prioridade na aquisição de itens, etc.

token infungível

❶ (abreviado NFT, “*non-fungible token*”) classe ampla de tokens em que cada unidade individual é considerada única, insubstituível, e, portanto, passível de valoração e preços próprios. Popularmente utilizado na tokenização de ativos digitais únicos, como arte digital, colecionáveis, propriedade virtual, itens de jogos, etc.

tokenização

❶ o processo de criar, em uma rede de criptomoedas, uma representação de algum ativo ou direito do mundo real, permitindo sua divisão, transferência, compra, venda ou gestão usando as características inerentes à criptomoeda (auditabilidade, descentralização, etc.)

tokenizadora

❶ pessoa jurídica que executa e gere a tokenização de determinados ativos, agindo como ponte entre o ativo original e sua versão tokenizada.

token não-fungível

❶ *mesmo que:* ➤ token infungível.

tokenomics

❶ (contração de “*token economics*”) área de conhecimento emergente que estuda as propriedades econômicas de tokens baseado em *blockchains*, tais como avaliar o valor que traz aos agentes econômicos, como criar e distribuir recursos escassos, como o sistema interage com outros processos econômicos externos, como os agentes econômicos se comportam mediante quais incentivos, etc.

trabalho

❶ procedimento computacional (calcular *hashes*, tipicamente) repetitivo e laborioso que despende grandes quantidades energia elétrica, espaço de armazenamento, ou outros recursos escassos, mas que, uma vez se tendo o resultado, é barato, rápido e fácil de auditar que está correto. ❷ medida da quantidade de trabalho realizado até então.

📖 *A quantidade de trabalho do bloco gênese do Bitcoin foi por volta de 4,3 gigahashes.*

trader

❶ (“negociador”) aquele que busca ganhar dinheiro (em *fiat*, tipicamente) com operações de curto prazo através da compra e venda de ativos financeiros, aproveitando-se da volatilidade dos preços.

📖 *Apesar de ser uma profissão “abominada” por muitos (principalmente os mais leigos sobre finanças), o trader é fundamental para o funcionamento do mercado, pois ele é quem ajuda a “precificar” os ativos no curto prazo, além de dar liquidez ao mercado.*

transação

❶ conjunto de informações que descrevem a ocorrência de certos eventos, como a criação de unidades monetárias, transferência dessas unidades monetárias, as condições para que essas transferências possam ocorrer, a satisfação dessas condições, ou a notarização de dados arbitrários.

troca atômica

❶ um dentre diversos possíveis esquemas para realizar trocas entre duas criptomoedas diferentes, ou tokens residindo em redes distintas, de forma atômica (sem possibilidade de um dos lados sair prejudicado), de forma direta entre as partes, sem intermédio de um “terceiro confiável”, tal como uma corretora.

📖 *Conta a lenda que a primeira troca atômica entre Bitcoin e Litecoin foi em setembro de 2017.*

USD

❶ abreviatura de “dólares americanos” (United States Dollar), a moeda nacional dos Estados Unidos, segundo o padrão ISO 4217.

USDT

❶ abreviatura da stablecoin “Tether”, com o prefixo “USD” indicando que ela espelha o



valor do dólar americano, e o “T” representando o “Tether” (“coleira”, em português).

utility token

① *mesmo que:* • token de utilidade.

valor mobiliário

① instrumento financeiro representativo de um valor monetário, ou de um direito, negociável em mercados financeiros. Inclui ações, debêntures, notas promissórias, opções, futuros, ou quaisquer outros títulos ou contratos de investimento ofertados publicamente que gerem direito de participação, parceria ou remuneração, cujos rendimentos advêm do esforço de um empreendedor ou de terceiros.

verificação de pagamento simplificada

① (em inglês, “simple payment verification”, frequentemente abreviado “SPV”) técnica descrita no whitepaper original do Bitcoin para, usando as árvores de Merkle, confirmar a existência de um pagamento baixando menos de um milésimo do tamanho total do blockchain (que tipicamente tem várias centenas de gigabytes), viabilizando a existência de carteiras nativas de Bitcoin mesmo em dispositivos com pouca capacidade de armazenamento, tais como telefones celulares.

wei

① unidade de conta equivalente a 0,000000000000000001 (10^{-18}) ether, que é a menor quantidade representável.

web1

① os primeiros anos da internet, em que os sites eram primariamente texto, com pouca interatividade ou capacidade de geração de conteúdo pelo usuário final.

web2

① a segunda era da internet, caracterizada pela participação ativa dos usuários finais, com o surgimento de blogs, vlogs, wikis, redes sociais, smartphones & apps, etc.

web3

① uma visão para o futuro da internet, ainda em construção, para o qual se prevê a convergência de tecnologias como redes baseadas em blockchains, inteligência artificial, com os usuários tendo controle completo sobre seus próprios dados através de sistemas mais descentralizados.

whitepaper

① um artigo detalhando a proposta de um projeto, sistema, criptomoeda, produto ou serviço, descrevendo suas bases técnico-científicas, enfatizando seus benefícios,

invocações, explicitando as abordagens que adota e os problemas que resolve, o ambiente competitivo onde se insere, etc., a fim de ajudar potenciais investidores, usuários, reguladores, ou o público em geral, a avaliar seu mérito e valor.

XBT

❶ abreviatura de bitcoin, a unidade de conta, aderente ao padrão ISO 4217, que exige que códigos de moedas não-nacionais começam com “X” (“eXperimental”). *Contraste com:* ➤ BTC.



abcripto*

Rua Ramos Batista, 444 / 7º andar
Vila Olímpia, SP, 04552-020
São Paulo - SP

contato@abcripto.com.br



 abcripto.com.br

 [linkedin.com/abcripto](https://www.linkedin.com/company/abcripto)

 [@ABCriptoOficial](https://twitter.com/ABCriptoOficial)

 [@abcripto](https://www.instagram.com/abcripto)

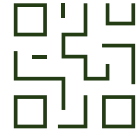


Soluções estratégicas em economia

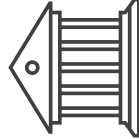


Panorama setorial da criptoeconomia no Brasil

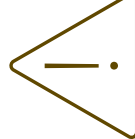
Outubro de 2022



Governos em todo o mundo observam a revolução dos criptoativos e o surgimento da criptoeconomia; disrupção e criação de novas formas de geração de valor provocam amplas discussões regulatórias e tributárias



- No Brasil, a Instrução Normativa 1.888/2019 da Receita Federal do Brasil constituiu um importante avanço na regulação de transações de criptoativos
- Debate atual sobre um marco regulatório mais abrangente para a criptoeconomia, como proposto no Projeto de Lei (PL) 4.401/2021

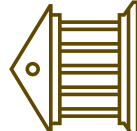


O atual mercado de intermediação de criptoativos é caracterizado pela presença de diferentes modelos de negócios de exchanges

Construção de um ambiente seguro e regulado pode ser crucial para o desenvolvimento da criptoeconomia no Brasil

Propostas de marco regulatório, como o **PL 4.401/2021**, visam discutir questões relacionadas à:

Autoridade de cada órgão para regulação, fiscalização e tributação de transações com criptoativos



Segurança do patrimônio dos usuários e coibição de práticas ilegais



Redução da assimetria regulatória entre *exchanges* com e sem domicílio fiscal no Brasil



Análise tributária e regulatória deste trabalho concentra-se em transações públicas (intermediação e saque) em exchanges



- Não compreende transações P2P, em OTCs, DEX e serviços de tokenização
- Restrição da análise decorre da dificuldade de identificação destes agentes e operações através de dados públicos

-
- ▶ **Contextualização**
 - ▶ **Criptoativos e Criptoeconomia**
 - Conceitos
 - Potencias desdobramentos da criptoeconomia
 - ▶ **Exchanges de criptoativos**
 - ▶ **Criptoeconomia e exchanges no Brasil**
 - ▶ **Desafios regulatórios**
 - Panorama regulatório internacional
 - Estado regulatório em jurisdições selecionadas
 - Histórico regulatório no Brasil
 - Projeto de lei em discussão no Brasil - PL 4.401/2021
 - ▶ **Tributação das exchanges de criptoativos**
 - Referências internacionais – OCDE (2020)
 - Estimativa de potencial arrecadatório das exchanges que contribuem atualmente
 - Cenários de conformidade tributária das demais exchanges
 - ▶ **Anexos**

Criptoativos e criptoeconomia



Histórico

Em **2008** foi criado o **bitcoin** com o objetivo de permitir transferências diretas sem a necessidade de intermediação

- A moeda foi a primeira introdução a tecnologia *blockchain*, uma aplicação da *Digital Ledger Technology* (DLT)
- DLTs são bancos de dados geridos por diversos participantes, de forma transparente e não centralizada

Deste modo, bitcoin é o primeiro **criptoativo**

FMI: “Criptoativos são representações digitais de valor, criados com utilização de criptografia, a partir de tecnologia de registro eletrônico distribuído”¹

Criptoativos se distinguem por diversos atributos, tais como:

- tipo de *blockchain* utilizado;
- formas de autenticação/mineração e custos envolvidos;
- restrições de emissão;
- **utilidade econômica.**

1 . Fonte: Sexta edição do Manual de Balanço de Pagamentos e Posição de Investimento Internacional (BPM6) do FMI.

Nota: Vide Anexo I para mais definições e conceitos

Classificação de Tokens

Criptoativos também são **tokens**² (conceito mais amplo)

Para estabelecer um arcabouço regulatório, agências internacionais (como a OCDE) classificam *tokens* em **categorias amplas**, de acordo com sua **utilidade econômica**:



Meio de pagamento

Payment/Exchange Tokens



Atribuição de Posse

Non-fungible Tokens



Securitização

Security/Equity Tokens



Atribuição de direitos

Utility Tokens



Problemas da Classificação de Tokens



Classificação não abrange todos os criptoativos – como exemplo, documentos



Alguns *tokens* podem se inserir em mais de uma dessas categorias - *tokens* híbridos



Tokens classificados dentro das categorias mencionadas podem ter **funções diversas**

2. Sequência de caracteres que constitui uma representação criptográfica de um conjunto de direitos e ser utilizado dentro de um contexto específico. Não são originalmente monetários.

BLANDIN, A. et al. Global Cryptoasset Regulatory Landscape Study. University of Cambridge, Centre for Alternative Finance, 2019.

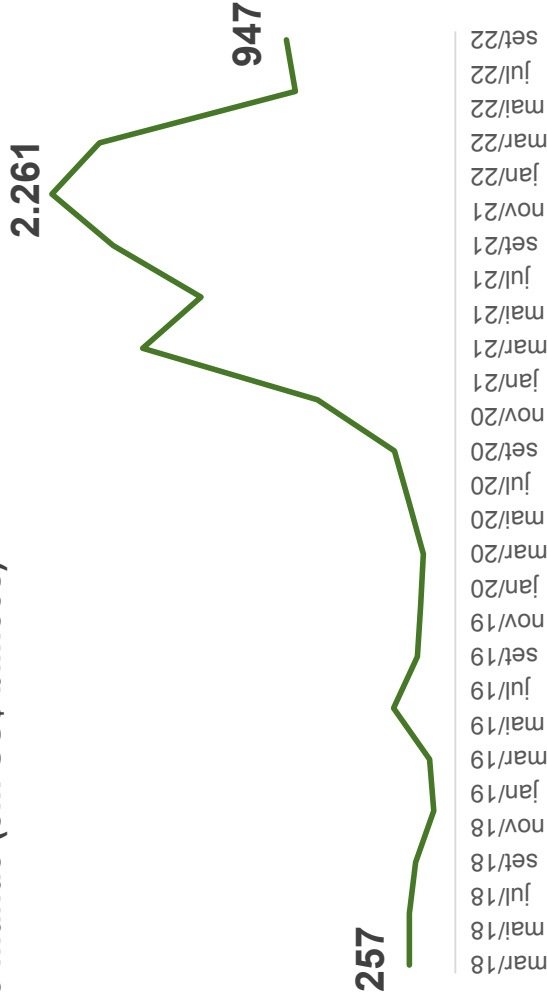


Valor de Mercado

Valorização de criptoativos de maior proeminência, como bitcoin (301% de mar/18 a mar/22) e ether (303%), bem como surgimento de centenas de novos criptoativos

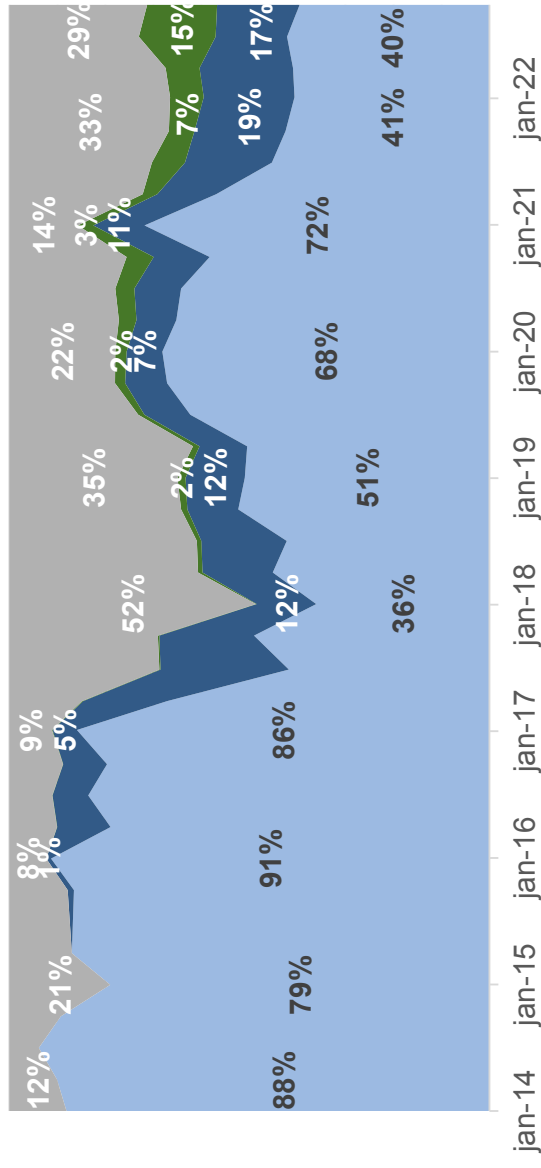
Desenvolvimento tecnológico, novas aplicações e maior demanda por ativos de risco são fatores explicativos do expressivo crescimento observado pós-2020

Evolução do valor capitalização de mercado dos criptoativos no mundo (em US\$ bilhões)



Fonte: CoinMarketCap. Elaboração: LCA Consultores.

Participação no valor de capitalização de mercado, por criptoativo



Nota: As stablecoins consideradas foram as de maior capitalização em jan/22: Tether, USD Coin e Binance USD. Fonte: CoinMarketCap. Elaboração: LCA Consultores.

Bitcoin ainda é predominante, mas há crescente diversificação dentre os criptoativos

- Rede **Ethereum** surge a partir de 2016, e **stablecoins** aumentam em proeminência a partir de 2020

É possível observar, dois movimentos simultâneos:

- Expansão das transações e do uso de criptoativos;
- Diversificação dos tipos de criptoativos existentes, bem como de suas respectivas funções.

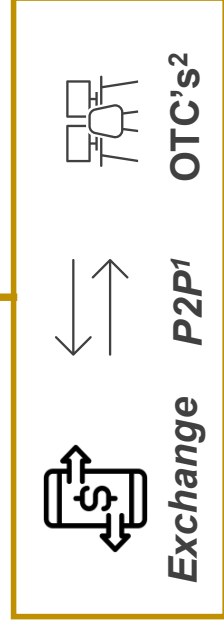
Meio de troca utilizado como **meio de pagamento**. Tipologia abrange:

- **Criptomoedas não lastreadas:** ativos sem contraparte devedora, emissor e promessa de retorno, quando utilizados como ativos de investimento podem ser considerados ativos híbridos (como o bitcoin e o ether)
- **Criptomoedas lastreadas:** *Stablecoins* (ativos pareados com moedas fiduciárias) e *CBDCs* (*Central Bank Digital Currency*, moedas digitais criadas em *blockchains* privados por bancos centrais)



Operações e agentes que envolvem criptomoedas

Transações



Usuários



Custodiantes

Provedores de Liquidez
(*Market-Maker*)



Mineração

Autenticação

1. P2P

- ✓ Formato original de transação de criptoativos, via *blockchain* sem a presença de intermediários

2. Over the Counter (OTC)

- ✓ Compras e vendas são acordos bilaterais, não públicos, para blocos maiores de operações



Usuários



Complexidade tributária

Diferentes classificações de ativos e formas de transações levam a incidências tributárias distintas



De acordo com a Anbima, a transformação de ativos “físicos” ou “reais” em ativos digitais é chamada de *tokenização*

Ativos reais



Ativos únicos

Ex.: Obras de arte



Direitos

Ex.: Participação em tomada de decisão



Propriedade

Ex.: Participação em receitas de ativos

TOKENIZADORAS



NFT

São representações digitais de **ativos únicos**, não trocáveis, como obras de arte
Representam propriedade desses itens, mas não são instrumentos de investimento

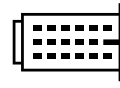


Utility Tokens

Permitem **acesso a produtos**, plataformas ou serviços digitais específicos

Tokens podem permitir acesso a votações e outros processos de tomada de decisão

Ex: *Fan Tokens* ou *tokens* de governança



Security ou Equity Tokens

Representam **títulos de propriedade e instrumentos de investimentos**

Possibilitam ao emissor captar recursos e dão direito a remuneração ao seu detentor, de modo análogo a ações

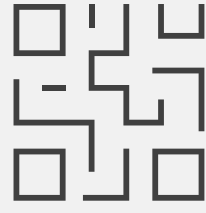


Tokenizadoras

- Funcionam como agentes “estruturadores” do mercado de criptoativos
- Processo de tokenização permite a venda de direitos e recebíveis que de outro modo seriam ilíquidos
- No Brasil, são obrigados a declarar à Receita fatos relativos à emissão de criptoativos (pela IN 1.888/2019)
- Discussão sobre tributação é complexa, havendo no Brasil **possibilidade** de incidência de:
 - ICMS pela posse e emissão de ativos que conferem acesso a mercadorias
 - IOF por tokenização de debêntures
 - ISS e PIS/Cofins na prestação de serviços de tokenização

Mercados da criptoeconomia estão em pleno desenvolvimento e apresentam **características disruptivas que trazem novidades e incertezas** quanto a:

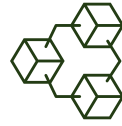
- Formas de geração de **valor**
- **Responsabilidade** de cada agente sobre as transações
- Possibilidades e desafios **regulatórios**, dentre outros



Variações extremas de mercado são muito frequentes, de modo que agentes “líderes de mercado” são inconstantes



Anonimato da posse e não rastreabilidade das transações torna o sistema vulnerável a ser usado para acobertar atos ilícitos. Regulação adequada é a solução típica de minimizar esse risco



Desdobramentos da criptoeconomia para os demais setores da economia são **incertos**, mas vislumbra-se o uso da tecnologia *blockchain* em diversos setores

Outras aplicações das tecnologias de *blockchain* e tokenização estão em desenvolvimento, algumas já podem ser encontradas no setor público e privado



Cadeia de suprimentos

Tecnologia de *blockchain* pode garantir a procedência de alimentos, promovendo informações como: local de produção, percurso dos alimentos, agrotóxicos, remuneração dos empregados, dentre outras



Uso de plataforma pecuária transparente para monitoramento de desmatamento e uso de mão de obra nos locais de produção¹



Rastreamento de produtos e lotes, sobretudo em parceria com a rede Walmart². atualmente atuante cadeia do café, pesca, dentre outras³



Digitalização Segura

Redes em *blockchain* também podem ser utilizadas por governos e empresas visando modernização do processo de registros

Receita Federal – Rede em *blockchain* em fase de testes facilita compartilhamento e autenticidade de dados do CPF e CNPJ⁴

Governo do Ceará – *Blockchain* para registro e monitoramento de transações em obras públicas⁵

Governo estima economizar ~2% do PIB/ano com assinaturas digitais em *blockchain*, através da redução de custos cartoriais⁶

Referência em **identificação digital** e armazenamento de informações relativas a **saúde**



Brasil



Estônia



CBDCs

Instrumento de pagamento digital, denominado na unidade nacional de conta, que constitui um passivo do Banco Central

Podem oferecer novas capacidades e possibilitar transações em moeda análoga à fiduciária sem intermediários financeiros:

- **Maior eficiência de pagamentos:** Potencial de se oferecer meios de pagamentos com baixo custo como um bem público
- **Estímulo à competição e à diversificação** de ativos financeiros e meios de pagamento

1. <https://jbs.com.br/saiba-mais/blockchain/>; 2. <https://www.hyperledger.org/learn/publications/walmart-case-study>; 3. <https://www.ibm.com/br-pt/blockchain/solutions/food-trust>; 4. <https://www.serpro.gov.br/menu/Imprensa/Releases/serpro-desenvolve-rede-blockchain-para-a-receita-federal>; 5. <https://www.ceara.gov.br/2020/10/27/governo-do-ceara-investe-na-tecnologia-blockchain-para-medicao-de-obras/>; 6. <https://epocanegocios.globo.com/Tecnologia/noticia/2018/08/como-estonia-construiu-uma-sociedade-digital.html>

Exchanges de criptoativos



Realizam transações públicas e transparentes, em um livro de ordens análogo a um mercado tradicional

Plataformas que atuam como **intermediárias** em transações de criptoativos, se apresentando como alternativas às negociações P2P, sobretudo por:

- Capacidade de redução dos custos de transação;
- Redução de assimetria de informação pela garantia às partes envolvidas que as operações serão liquidadas

Serviços das exchanges

Principais serviços oferecidos pelas **exchanges**:

- Venda direta é organizada através da compra/venda de criptoativos de *market-makers* e outros agentes, ligando-os aos clientes;
- Intermediação conecta dois clientes, ofertando o serviço de *matching* entre comprador e o vendedor;

Venda direta e intermediação

Parte das receitas das **exchanges** advém de taxas cobradas sobre transações (ordem)



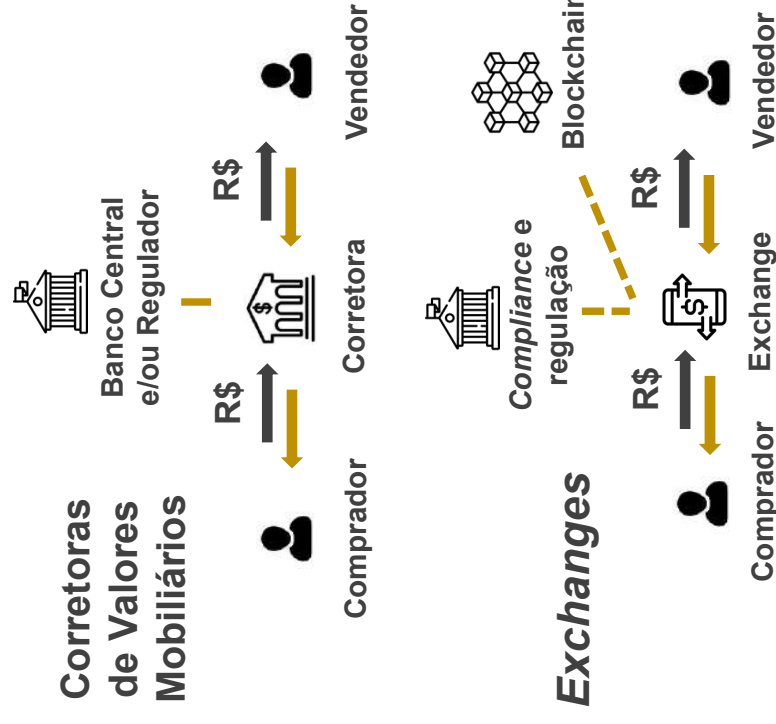
Armazenamento

Função realizada por **custodiantes e exchanges**, permitindo compra e venda utilizando carteiras próprias

Modelos de negócio

Maioria das plataformas são **centralizadas**, funcionando de maneira semelhante a uma corretora de valores mobiliários

- Plataformas **descentralizadas (DEX)** operam através de um protocolo de *smart contracts* na *blockchain*





Dentre as exchanges com maior *share* mundial (em volume transacionado), grande parte tem **sede em paraísos fiscais ou países com regime fiscal privilegiado**¹

10 maiores exchanges do mundo, por *exchange score* (sedes entre parênteses)



(Ilhas Cayman)



(Seychelles)



(Bahamas)



(Estados Unidos)



(Estados Unidos)



(Seychelles)



(Estados Unidos)



(Ilhas Virgens)



(Estados Unidos)



(Japão)

Data de referência: 25/07/2022. Fonte: CoinMarketCap.

1. Segundo definição da Instrução Normativa N° 1037, de 04 de junho de 2010 Ilhas Cayman, Bahamas, Hong Kong e Seychelles são paraísos fiscais, enquanto Malta é um regime fiscal privilegiado para: International Trading Company (ITC) e de International Holding Company (IHC). 2. Estão em discussão propostas que enderecem o tema, visando especificamente facilitar a tributação da economia digital.



Mercado possui **elevada volatilidade**, de forma que o volume por *exchange* pode apresentar flutuações significativas diariamente



EUA tem condicionado operações de grandes *exchanges* à presença de **sedes locais**, que se comportem de acordo com a regulação local (caso da Binance US)

Exchanges internacionais e paraísos fiscais

Problemática envolvendo *exchanges* em paraísos fiscais **não é restrita ao Brasil**

- Regulação nacional, porém, tem espaço para aprimoramentos no combate a este problema

- Prática **não é ilegal** mas promove **assimetria concorrencial**

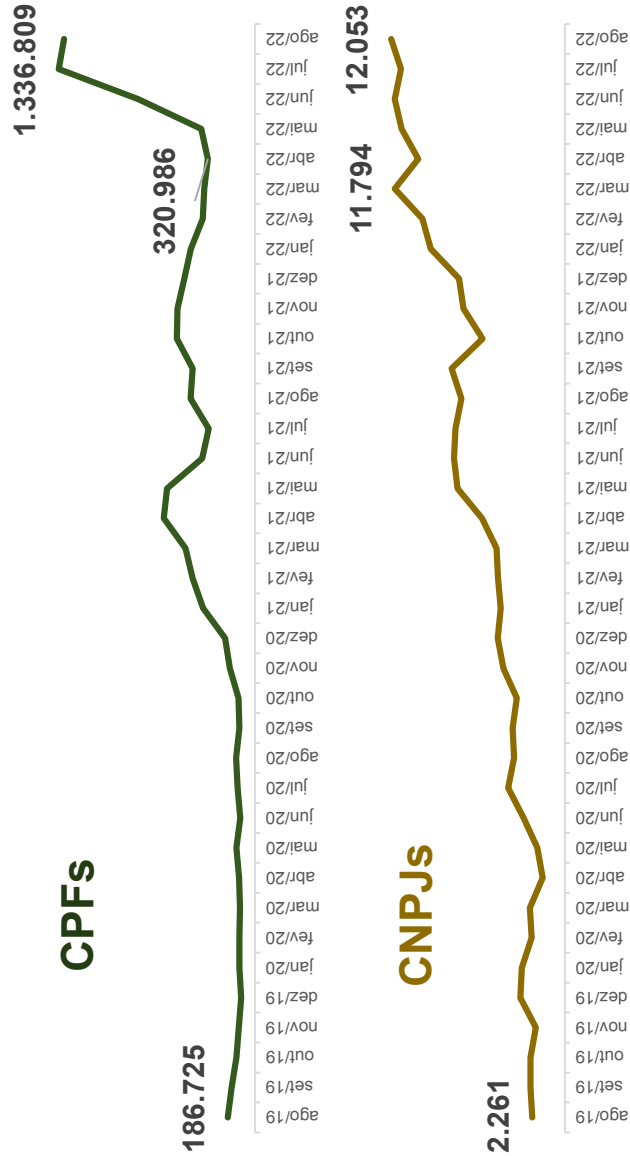
Tributação por presença econômica relevante é recomendação da OCDE contra práticas de *profit shifting* ou transações trianguladas, permitindo atrair competência tributária para o Brasil²

Criptoconomia e exchanges no Brasil

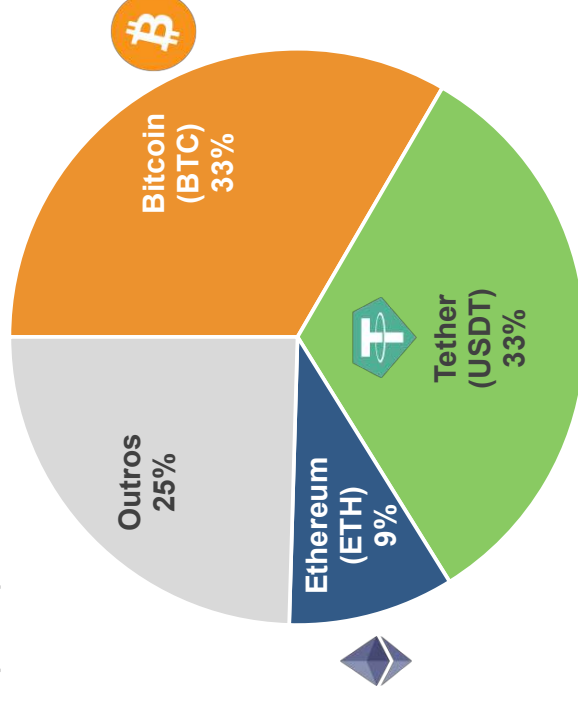


Segundo informações declaradas para a Receita Federal do Brasil, mercado **creceu de modo expressivo**, incluindo cada vez mais pessoas e empresas, sobretudo a partir de 2020

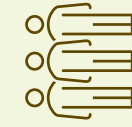
Número de CPFs e CNPJs únicos declarantes de negociações com criptoativos (em milhares)



Proporção, por criptoativo utilizado, do valor transacionado declarado (2021)



Nota: "Outros" inclui demais criptoativos declarados para a RFB (como USDC, CHZ, dentre 60 outros). Fonte: Receita Federal do Brasil. Elaboração: LCA Consultores.

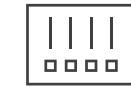


- **Perfil dos detentores de criptoativos**
- **Estudo da TripleA¹ estima que 5% da população do Brasil (10,4 milhões) possui criptoativos**
- **87% das operações em criptoativos no Brasil em 2021 foi feita por pessoas do sexo masculino**

1. TripleA (2021) Cryptocurrency across the world.

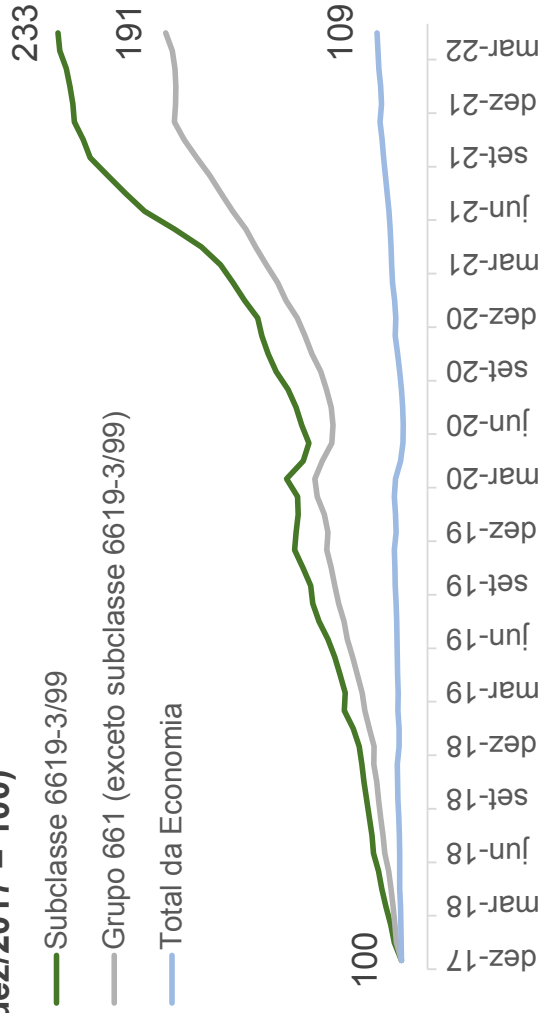


Há indícios de geração significativa de empregos em empresas nacionais de criptoeconomia



A **CNAE 6619-3/99**, “Outras atividades auxiliares dos serviços financeiros não especificadas anteriormente”, engloba, entre outras atividades, **custódia e cessão temporária (locação) de criptoativos**¹

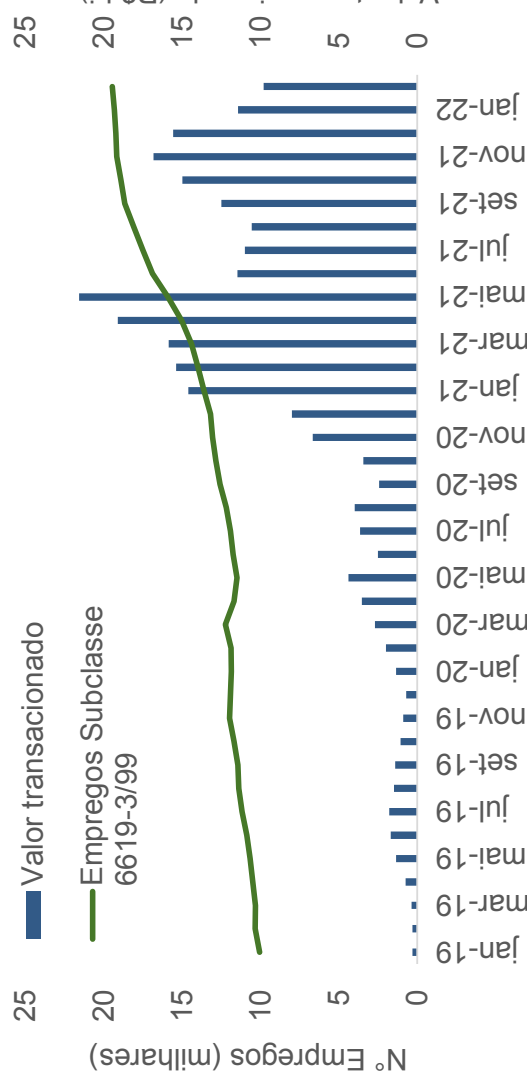
Evolução comparada do número de vínculos empregatícios (dez/2017 = 100)



Nota: Os dados da CNAE grupo 661 excluem a subclasse 6619-3/99 para esclarecer a comparação entre as atividades. Fontes: CAGED e RAIS. Elaboração: LCA Consultores.

1. A CNAE 6619-3/99 engloba: casas de câmbio, plataformas de pagamento online, corretagem de consórcios, corretor hipotecário, além de serviços de corretagem, custódia e cessão temporária (locação) de criptoativos. O Grupo 661 “Atividades auxiliares dos serviços financeiros” é o que engloba a subclasse em questão, por isso a comparação com o mesmo pode mostrar de que forma o mercado cripto se destacou de atividades comparáveis.

Comparação da evolução de vínculos da CNAE 6619-3/99 com o valor de criptoativos transacionados por exchanges no Brasil



Fontes: CAGED, RAIS, CoinTradeMonitor e RFB. Elaboração: LCA Consultores.



Entre jan/19 e fev/22, o nº de empregos da CNAE 6619-3/99 **dobra em magnitude**, com geração de cerca de **10 mil empregos** nesta CNAE

Tal cenário coincide com o período de **maior crescimento das transações com criptoativos** por brasileiros



Exchanges que atuam no mercado brasileiro pode ser segmentadas de acordo com os seus modelos de negócio



Nacionais

- Possuem domicílio no Brasil
- Vinte e seis exchanges



Nacionalizadas

- Possuem domicílio no Brasil, mas foram fundadas no exterior
- Duas exchanges



Parcialmente Nacionalizadas

- Possuem apenas empresas de intermediação financeira domiciliadas no Brasil
- Cinco exchanges



Estrangeiras

- Não possuem operações domiciliadas no Brasil
- Duas exchanges



Metodologia

Divisão entre exchanges construída a partir de pesquisa sobre os domicílios fiscais de cada exchange, considerando os locais de suas sedes, estrutura societária e se possuíam ou não CNPJ no Brasil (vide Anexo)¹

Para o cálculo de share, foram utilizados dados dos agregadores relativos a **transações totais de bitcoins**. Supõe-se que:

- 1) Transações são a melhor medida de participação de mercado;
- 2) Proporção de bitcoins por total de criptoativos transacionados é igual para qualquer exchange²

1. A Metodologia foi construída a partir de pesquisa sobre os domicílios fiscais de cada exchange, considerando os locais de suas sedes, estrutura societária e se possuíam ou não CNPJ no Brasil. Definições: (i) Nacional: Fundada no Brasil; sede no Brasil; CNPJ no Brasil; quadro societário composto exclusivamente por pessoas físicas e/ou jurídicas situadas no Brasil. (ii) Nacionalizada: Fundada no exterior; sede no Brasil; CNPJ no Brasil; quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. (iii) Parcialmente nacionalizada: Fundada no exterior; sede no exterior; CNPJ no Brasil como empresa de intermediação e com quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. (iv) Estrangeira: Fundada no exterior; sede no exterior; CNPJ no Brasil como empresa domiciliada no exterior ou ausente; quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. Classificação e discussão de casos especiais no Anexo.

2. Estimada 32,6%, média dos dados do Livecoins para o 2º semestre de 2021, período com informações completas de exchanges nacionais e internacionais.



Assimetria regulatória pode gerar distorções competitivas

EXCHANGES NO MERCADO BRASILEIRO



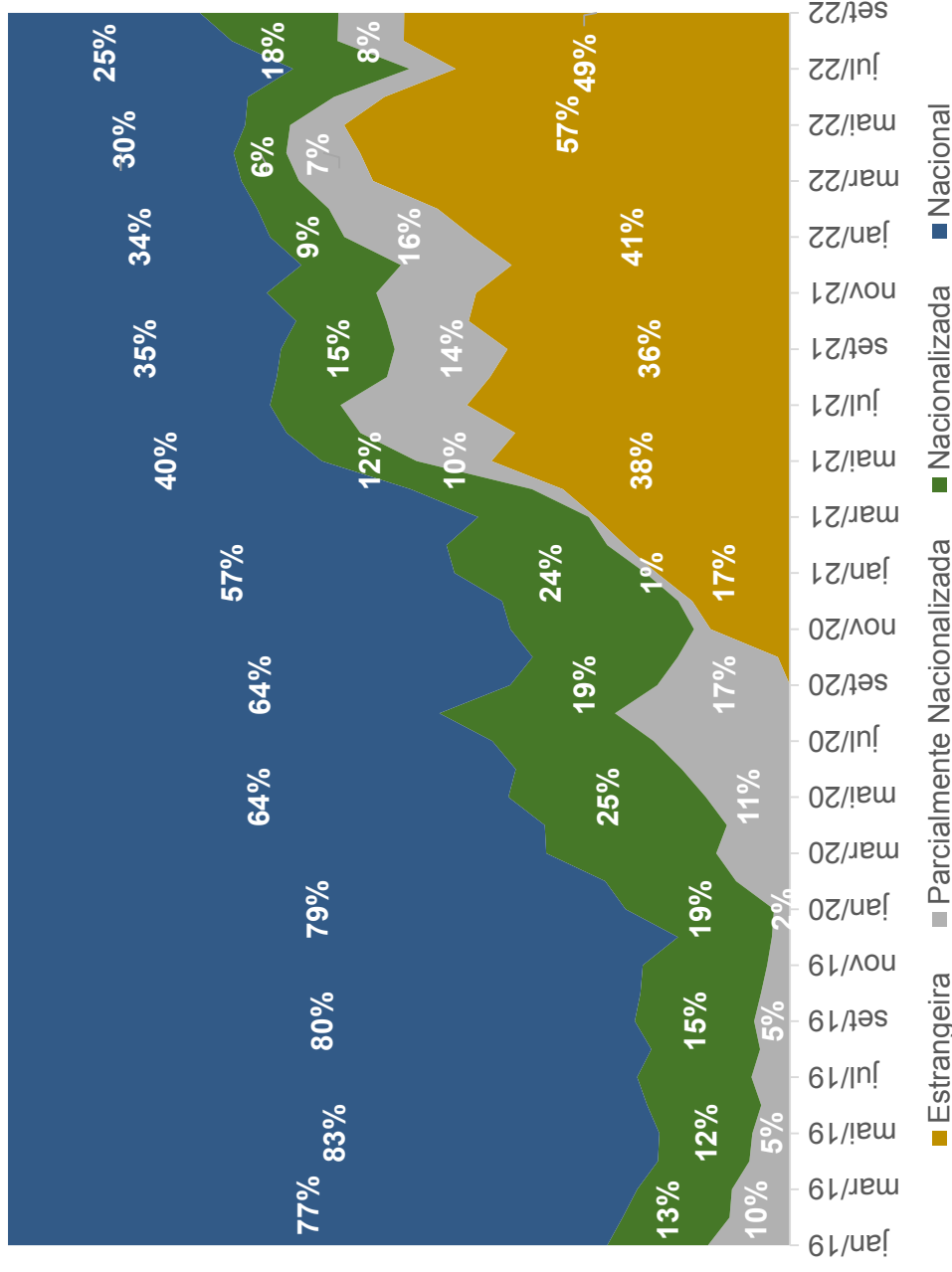
A partir de 2021 as exchanges estrangeiras passaram a constituir a maior parte do mercado brasileiro de bitcoin, com impacto significativo da entrada da Binance

Maiores exchanges de criptoativos no mercado brasileiro, por transações de bitcoin (2021)

	Exchange	Share	Sede
1º	BINANCE	30%	Ilhas Cayman*
2º	bitPreço	13%	Brasil
3º	MERCADO BITCOIN	13%	Brasil
4º	NovaDAX	12%	Brasil*
5º	Bitcoin <small>tayou</small>	9%	Seychelles*

* Estas exchanges apresentam circunstâncias específicas quanto à localidade da sede que são discutidas em Anexo.

Proporção de exchanges por classificação



Nota: Dados relativos a transações de bitcoins em exchanges. Fonte: CoinTrade Monitor. Elaboração LCA Consultores.

DIMENSIONAMENTO DE MERCADO - TRANSAÇÕES

Em 2021, foi **transacionado** no Brasil **R\$**



103 bilhões em bitcoin pelas *exchanges*¹

- Bitcoin representa 32,6% do valor total de transações criptoativos²



- Percentual referendo pelos dados da RFB (proporção média foi de 33,4% em 2021)

Valor total transacionado de criptoativos estimado em **R\$ 317 bilhões**, segmentado em:

- **R\$ 137 bi** por *exchanges* nacionais
- **R\$ 46 bi** por nacionalizadas
- **R\$ 29 bi** por parcialmente nacionalizadas
- **R\$ 105 bi** por estrangeiras



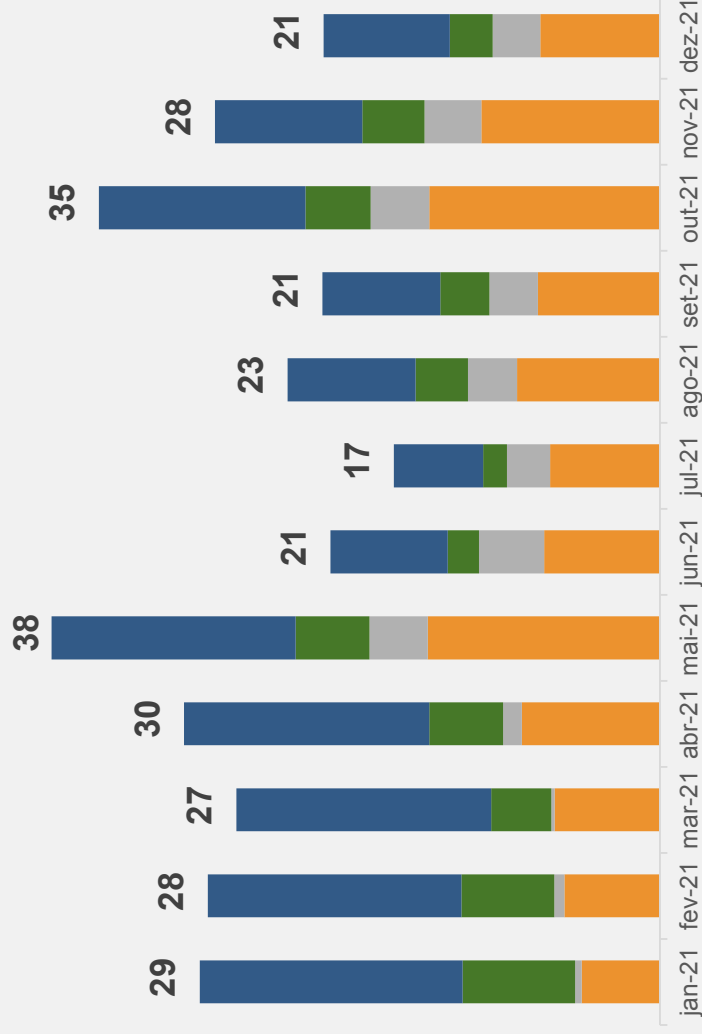
- Estimativa feita através da participação de mercado de cada *exchange*, utilizando dados de agregadores

1. Fonte: CoinTrade Monitor.

2. Média dos dados do Livecoins para o segundo semestre de 2021, período do ano com informações completas relativas as *exchanges*.

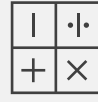
↔ Transações

Valor total de criptoativos transacionado no Brasil, mensal em 2021, por classificação de *exchanges* (em R\$ bilhões)



■ Estrangeira ■ Parcialmente Nacionalizada ■ Nacionalizada ■ Nacional

Fonte: CoinTrader Monitor e LiveCoins. Elaboração LCA Consultores.



Metodologia

Dado inicial: Saques em exchanges, de bitcoin em moeda fiduciária, no mundo¹ (não inclui operações entre exchanges)

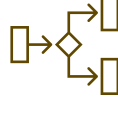
- Ajuste 1: Obter saques no mundo para total de criptoativos, não apenas bitcoin
- Premissa 1: Proporção de saques é igual dominância do bitcoin²

Estimativa intermediária: Saques em exchanges, de criptoativos, no mundo

- Ajuste 2: Obter dado apenas para o Brasil
- Premissa 2: Proporção de saques Brasil/mundo é igual à proporção de transações em exchanges Brasil/mundo³

Estimativa final: Saques em exchanges, de criptoativos, no Brasil

1. Dados em número de saques e valor total sacado. Fonte: CoinMetrics.
2. Dado de proporção de valor BTC/Total de criptoativos. Retirado do Messari.io.
3. Dado de transações em exchanges no Brasil estimado nesse mesmo estudo. Dado de transações mundiais em exchanges extraído do agregador Bitcoinity



Resultados

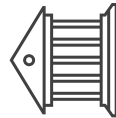
Para 2021 estima-se um total de **380.490 saques**, com valor total de **R\$ 85 bilhões**

- Desse valor, **R\$ 36 bi** foram sacados através de exchanges nacionais, **R\$ 28 bi** por meio de estrangeiras, **R\$ 12 bi** por meio de nacionalizadas e **R\$ 8 bi** por parcialmente nacionalizadas

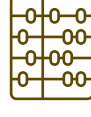
Saques de criptoativos em reais em exchanges, por divisão entre classificação de domicílio fiscal, em 2021

Exchange	N° de saques	Volume (mi)
Estrangeira	123.816	R\$ 28.124
Parcialmente Nacionalizada	33.957	R\$ 7.891
Nacionalizada	55.523	R\$ 12.254
Nacionais	167.193	R\$ 36.668
Total	380.490	R\$ 84.937

Fontes: CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA Consultores.



Banco Central do Brasil (BCB)



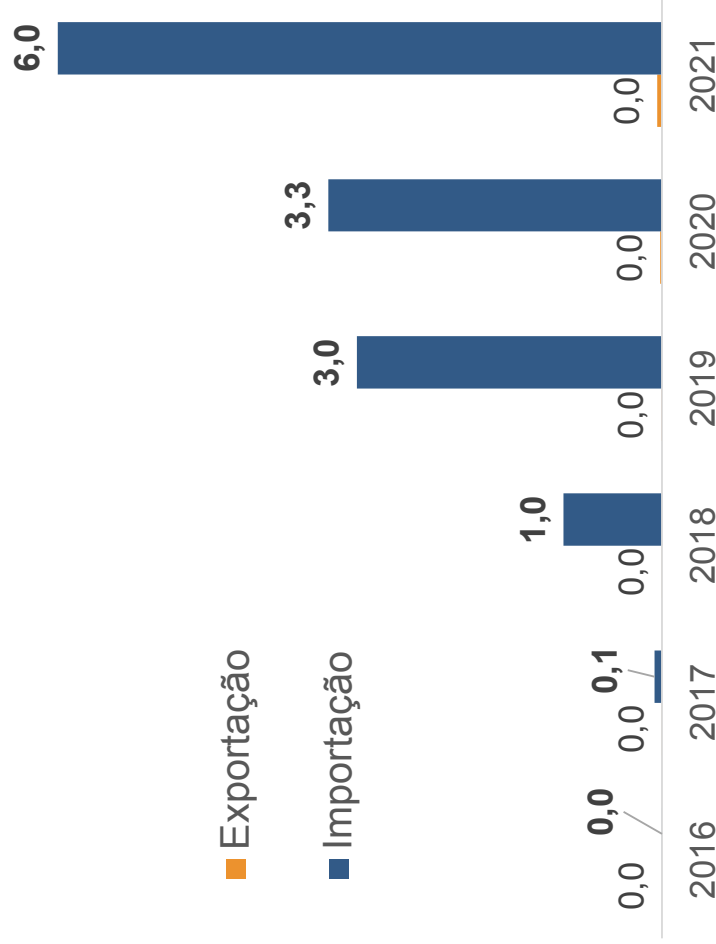
Metodologia de Estimação

BCB estima a importação e exportação de criptoativos através dos **contratos de câmbio em moeda fiduciária** entre as partes. Estimativas não captam transações entre criptoativos, observando **apenas ações de market-makers nacionais**

- Este número não contempla operações feitas entre criptoativos¹ de modo que a estimativa realizada pelo Bacen considera apenas parte das operações transfronteiriças

O valor total importado em 2021 é equivalente a **R\$ 32,2 bilhões**²

Estimativa do BCB de exportação e importação de criptoativos (em US\$ bilhões)



Fonte: Banco Central do Brasil. Elaboração: LCA Consultores.



Classificação

BCB, em acordo com diretrizes do FMI, classifica criptoativos como **ativos não financeiros** (porque não têm contraparte devedora) e incluem transferência de propriedade de criptoativos entre residentes e não residentes na **conta de bens do balanço de pagamentos**

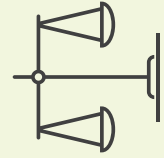
1. Supõe-se que agentes internacionais realizam operações utilizando apenas criptoativos. Esta premissa será relevante nas estimativas tributárias.
2. Conversão feita através da taxa de câmbio comercial média mensal (Banco Central do Brasil).

Desafios regulatórios

- I. Panorama regulatório internacional
- II. Estado regulatório em jurisdições selecionadas
- III. Histórico regulatório no Brasil
- IV. Projeto de lei em discussão no Brasil - PL 4.401/2021



Regulação de mercados financeiros traz ganhos aos consumidores ao **reduzir risco sistêmico, evitando crises com amplas consequências para a economia**¹



Inovação no mercado de criptoativos se beneficiaria através da **redução da assimetria de informação entre compradores e vendedores**, garantindo maior segurança aos usuários, em especial os ingressantes²



Recomendações de organismos multilaterais

- Organismos versam sobre a urgência de se estabelecer arcabouço internacional para regulação e tributação de criptoativos, especialmente considerando o **caráter transnacional de suas operações**
- Em abril/2022, OCDE publicou **padrão internacional para declaração de operações com criptoativos**, denominado CARF (*Crypto-Asset Reporting Framework*), normatizando as diretrizes já existentes e aumentando o escopo de atuação das autoridades tributárias, considerando os diversos tipos de intermediários (*exchanges*, operadores de carteiras, etc.)

1. *“É de particular importância que os governos utilizem a regulação para evitar a geração de risco sistêmico, de modo a evitar também futuras crises, que podem ser profundamente negativas para a economia real.[...] Está cada vez mais claro que uma regulação eficiente não é importante apenas para a economia real, mas também protege a estabilidade do próprio sistema financeiro e as instituições financeiras individuais.” Griffith-Jones (2010, pg. 106)*

2. *“While investors should be allowed to invest in risky assets, including cryptocurrencies, there should be adequate disclosure. This implies sound regulation of digital asset advertising by crypto platforms, which can often be misleading and downplay risks.” (BIS, 2022 pg. 88)*



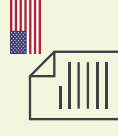
Tecnologia e mercado incipiente dificultam desenvolvimento regulatório

- Não há arcabouço de boas práticas regulatórias preestabelecido para criptoeconomia, podendo a legislação nacional se aproveitar de diferentes aspectos de cada jurisdição
- BIS: “Em todos os temas regulatórios, a natureza global da criptoeconomia e das DeFi requisitará cooperação internacional”¹



EUA

- Operação de exchanges de criptoativos é legal, mas deve se conformar ao **Bank Secrecy Act (BSA)**, submetendo relatórios às autoridades
- Após nov/2021, exchanges passaram a ser consideradas corretoras, **informando o órgão de Receita sobre as operações com criptoativos**
- Estabelece em mar/2022 diretrizes para **CBDC** americana, bem como definições para “ativos digitais”, “criptomoedas”, etc.
- *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps*²
 - Reconhece que a criptoeconomia pertence ao sistema financeiro e reforça sua importância regulatória



Proposta: Lummis-Gillibrand Crypto Bill³

- Prioridade: promoção de inovação aliada a proteção do consumidor
- Tem como objetivo segmentar criptoativos para órgãos que já possuem o *know-how* por regular ativos semelhantes
 - CFTC (regula *commodities*) – *tokens* descentralizados parecidos com *commodities*
 - FDIC (regula sistema bancário) – *stablecoins*
 - SEC (regula *securities*) – *tokens* de capitalização, como *utility tokens*

1. “Across all areas of regulation, the global nature of crypto and DeFi will require international cooperation” (BIS, 2022 pg 88). 2. Disponível em:

<https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf> (acesso em 30/08/2022). 3. Disponível em: <https://www.congress.gov/bill/117th-congress/senate-bill/4356/text> (acesso em 30/08/2022). Outras fontes: OCDE (2020) *Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues*; Comply Advantage (2022) *Crypto Regulation Around The World*.



União Europeia

- **Exchanges** de criptoativos são reguladas por diretrizes de cada Estado-membro, devendo se conformar à **compliance das autoridades financeiras europeias**
 - Em geral, ganhos de capital são taxados (alíq. 0-50%) e serviços prestados por **exchanges** são passíveis de tributação
- **DLT Pilot Regime**: Proposta de regulamentação que tem como objetivo fornecer um aparato legal para a infraestrutura de mercado de DLT¹
- Países asiáticos como Japão e Singapura tem seguido o modelo da União Europeia²



Regulation on Markets in Crypto-assets (MiCA)³

- Em junho de 2022, foi estabelecido um **acordo provisório pela aprovação da MiCA**
- Expectativa é que legislação cubra **gaps** regulatórios importantes, incluindo emissão, custódia e troca de criptoativos (exceto NFT)
 - Provedores de serviços precisariam de autorização para operar na EU e devem se responsabilizar pelos ativos
 - Stablecoins precisariam de reservas líquidas robustas; todas serão fiscalizadas pela autoridade bancária (EBA)
 - Autoridade de investimentos (ESMA) poderá desenvolver padrões técnicos para avaliar impacto ambiental dos ativos

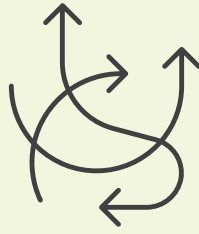
Comparativo entre legislações EUA e UE – Convergências e divergências



- **Convergências**: Segmentação regulatória entre órgãos existentes, destacando especialmente **stablecoins**, designadas para órgãos reguladores bancários
- **Divergências**: Legislação proposta nos EUA avança mais na classificação de ativos, sobretudo segmentando **securities** de **commodities**; legislação europeia se atenta mais à aspectos ambientais

1. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594> (acesso em 30/08/2022) 2 . Segundo apresentação institucional do Banco Central do Brasil;

3. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593> (acesso em 30/08/2022). Outras fontes: OCDE (2020) *Taxing Virtual Currencies: An Overview Of Tax Treatments And Emerging Tax Policy Issues*; Comply Advantage (2022) *Crypto Regulation Around The World* .



Dificuldades na definição do que é um criptoativo e de arcabouço regulatório específico a estes torna a **deliberação sobre o tema difusa** entre o Banco Central do Brasil (BCB), a Comissão de Valores Mobiliários (CVM) e a Receita Federal do Brasil (RFB)



BANCO CENTRAL DO BRASIL

2014
Moedas virtuais ≠ eletrônicas

2017
Alerta sobre riscos de moedas virtuais: não reguladas por nenhuma autoridade e sem lastro

2019
Criptoativos, considerados **ativos não-financeiros**, incluídos no balanço comercial (contratos de câmbio)

2021
Diretrizes para criação de uma CBDC, o “**real digital**”



Comissão de Valores Mobiliários

2018
Criptoativos ≠ ativos financeiros, não permitindo sua aquisição direta pelos fundos regulados; permite-se apenas investimento indireto através de ativos de outras jurisdições

2020
Regulamenta um “**sandbox regulatório**” para o mercado de criptoativos

2021
Autoriza o lançamento do **1º ETF de criptoativos** do mundo na B3, permitindo também mais fundos a investir em criptoativos

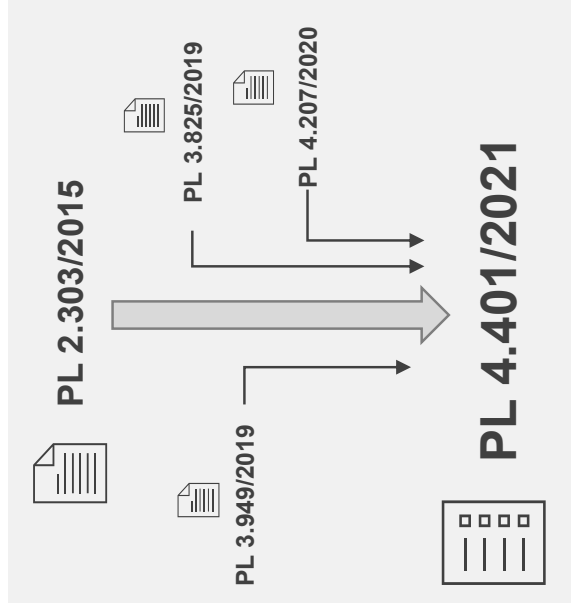


Receita Federal

2017
Criptoativos equiparados a ativos financeiros e sujeitos à tributação pelo ganho de capital, caso fossem vendidos em valor >R\$ 35 mil/mês

2019
IN 1.888/2019: obrigatório informar todas as operações de criptoativos por **exchanges** em território brasileiro e operações >R\$ 30 mil/mês em P2P ou **exchange** internacional

2022
Perguntas e respostas IRPF: Retira equiparação absoluta a ativos financeiros, restringindo-a as **stablecoins**



“Ativos Virtuais”

Representação digital de valor que pode ser negociada por meios eletrônicos e utilizada para pagamentos ou investimentos, **exceto**:

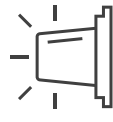
- Valores mobiliários;
- Moedas, inclusive eletrônicas;
- Instrumentos que provejam acesso a produtos ou serviços especificados, como NFT e *utility tokens*;
- Representações de ativos financeiros já regulados.



Prestadoras de Serviços de Ativos Virtuais

Definida como pessoa jurídica que executa, para terceiros, **por pelo menos um dos serviços de ativos virtuais**:

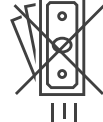
- **Troca** entre ativos virtuais e moeda, entre um ou mais ativos virtuais ou **transferência**;
- **Custódia** ou **administração**;
- Participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda



A prestação de serviços de ativos virtuais **deve obediência a diretrizes** como: manutenção de forma segregada dos recursos de clientes; proteção de dados pessoais; transparência nas operações e abordagem baseada em riscos



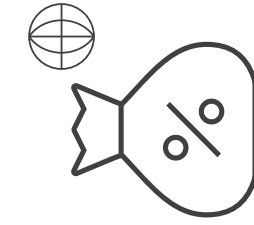
O órgão responsável pela supervisão das **exchanges** seria **definido posteriormente pelo Executivo**. O órgão teria como competência autorizar e suspender funcionamento de prestadoras de serviços de ativos digitais



Lei de Crimes Financeiros passa a prever a **necessidade de autorização prévia** para a prestação de serviços ligados a ativos virtuais, **obrigação que dificulta a operação de exchanges sem domicílio** no Brasil atualmente

Tributação de *exchanges* de criptoativos no Brasil

- I. Referências internacionais – OCDE (2020)
- II. Estimativa de receita tributável de *exchanges* nacionais e nacionalizadas
- III. Estimativa de parte da arrecadação atual do setor
- IV. Cenário de internalização das demais *exchanges*



Criptoativos, em geral, são considerados uma forma de tributação de ganhos de capital. Porém, os mesmos podem ser considerados ativos intangíveis (França), mercadorias (Áustria), instrumentos/ativos financeiros (Japão) ou moeda estrangeira (Itália)

Geralmente, **trocas** entre *tokens* de pagamento ou entre *tokens* de *pagamento* e moedas fiduciárias **não geram valor adicionado para** propósitos de tributação (decisão de Heqdvist na União Europeia)



Exchanges

- Quanto a **prestação de serviços** envolvendo criptoativos, estes são tipicamente considerados passíveis de incidência de Imposto de Valor Adicionado (IVA), possuindo **tratamento equivalente ao de intermediadoras financeiras**
- O IVA, porém, não é cobrado em muitos países (especialmente na União Europeia) por estarem sujeitos à mesma isenção de demais serviços financeiros

+ Possibilidades adicionais de incidência tributária

Relatório da OCDE também versa sobre tributação de **outras atividades** da criptoeconomia; entretanto há discordâncias dentre os países da organização de qual seria a incidência tributária ideal



Pode-se destacar como tributáveis sobretudo as **atividades de mineração e armazenamento**



ARRECADAÇÃO ATUAL – EXCHANGES NACIONAIS E NACIONALIZADAS

Através dos dados públicos disponíveis (volume de transações e taxas cobradas) é possível estimar a arrecadação de tributos que incidem sobre as exchanges



Dados só permitem estimar parte do faturamento das exchanges, tornando a análise parcial

Os slides seguintes apresentam as metodologias de cálculo, premissas e resultados segmentados por base de incidência tributária¹



Estimativa de arrecadação por incidência tributária, por participação no total estimado (2021)

Arrecadação estimada total



■ PIS/Cofins e ISS ■ IRPJ e CSLL ■ IOF

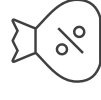
Fonte: Coin Trader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcoinity e BCB.
Elaboração LCA Consultores.

1. O Anexo VII apresenta o exercício exemplificando-o para uma exchange fictícia.

Faturamento
Estimado das
Exchanges



R\$ 985 Mi



Recolhimento de
PIS/Cofins e ISS

R\$ 85 Mi



Recolhimento
de IRPJ e CSLL

R\$ 107 Mi



Lucro
Presumido

R\$ 315 Mi



Importação
de Cripto



R\$ 32,2 Bi

Recolhimento
de IOF

R\$ 122 Mi



Arrecadação
estimada total



R\$ 314 Mi



Exchanges de criptoativos sofrem incidência de tributos sobre receita (PIS/Cofins e ISS), sobre lucro (IRPJ e CSLL) e sobre operações cambiais (IOF), dentre outros, sendo necessário estimar as bases de incidência

Estimativa de arrecadação potencial de exchanges de criptoativos

1. A partir do tamanho do mercado – em termos de transação e de saques – estima-se o faturamento tributável das *exchanges* nacionais e nacionalizadas a partir da aplicação das taxas cobradas
 - Taxa de **ordem**, cobrada como % do valor da transacionado
 - Taxa de **saque**: valor fixo por saque e/ou % sobre valor sacado

Obs: Exchanges possuem outras fontes de receita, não incluídas nesta estimativa por não constarem em bases de dados públicas
2. Sobre o faturamento são aplicadas as alíquotas dos tributos sobre prestação de serviços e sobre renda corporativa
 - Supõe-se que 100% das *exchanges* nacionais e nacionalizadas identificadas contribuem
3. Adicionalmente, estima-se a arrecadação sobre operações cambiais, através dos dados de importações de criptoativos (BCB)

Valores se referem ao ano de 2021



Outras possibilidades de incidência tributária

Há arrecadação de **outros tributos** ligados ao setor (IRPF, recolhimento sobre a folha de pagamentos, aquisição de insumos etc.), **tornando esta estimativa parcial**

Potencial arrecadatório em diversos agentes e operações **não tratados neste estudo**, como:



Tokenizadoras:

Incidência de ISS, ICMS e tributos sobre renda

OTCs e Custodiantes:

Incidência de ISS e tributos sobre renda corporativa





Metodologia

Mercados sobre os quais as taxas incidem são dimensionados na seção anterior, pelas equações¹:

$$Receita_{ordem} = taxa_{média} * transações_{exchanges_br}$$

$$Receita_{saque} = taxa_{média} * saques_{exchanges_br}$$

Taxas compiladas pelo agregador CoinTrade Monitor² a partir de informações coletadas junto a cada *exchange*, em maio/2022³:

↔ Média ponderada da taxa de ordem (*taker*) conforme o *market share* de cada *exchange* em 2021 – **0,43% para as nacionais e nacionalizadas**

📁 Média ponderada das taxas de saque fixa e variável conforme o *market share* de cada *exchange* em 2021 – **R\$ 5 e 0,40% para nacionais e nacionalizadas⁴**

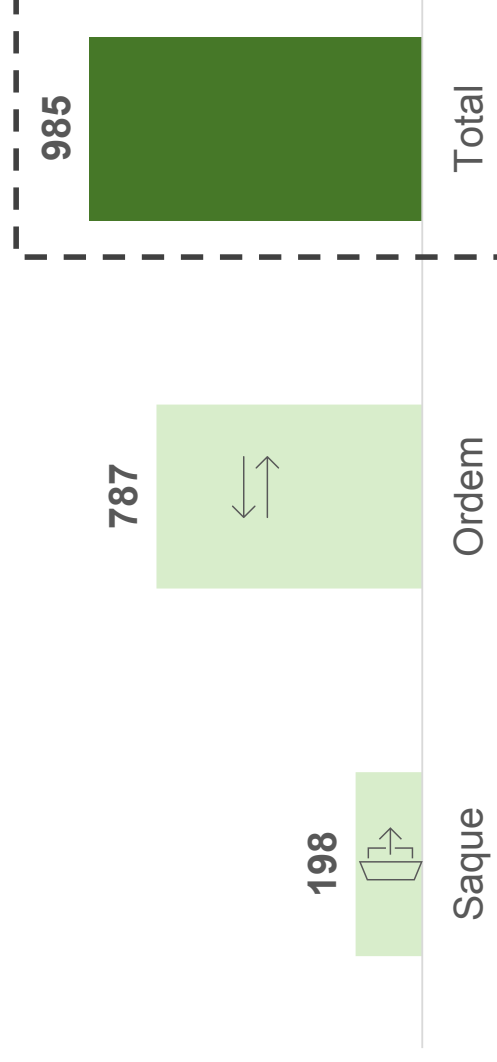
1. Mercado considerado é apenas o das *exchanges* nacionais.
2. <https://cointradermonitor.com/taxas-exchanges> acesso em Maio/2022
3. Vide anexo para detalhes.
4. *Exchanges* incluem nas taxas os tributos pagos, de forma que o faturamento estimado já compreenderia o recolhimento tributário estimado

Estimativa de faturamento das exchanges, em R\$ milhões, em 2021

	Ordem	Saques
Valor (ordem e saque) (A)	R\$ 183.552,5	R\$ 48.922,5
Número de saques (B)	-	222.716
Taxas médias (C)	0,43%	0,40% e R\$ 5,00
Faturamento das exchanges (A*C + B*C)	R\$ 787,3	R\$ 196,90 + R\$ 1,1 (R\$ 198,0)

Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity.
Elaboração LCA: Consultores.

Estimativa de faturamento das exchanges (R\$ mi 2021)



Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity.
Elaboração: LCA Consultores.

TRIBUTOS SOBRE PRESTAÇÃO DE SERVIÇOS

Tributo

Competência

Incidência

Alíquota

Observações e premissas

PIS/Cofins

Federal

Bens e serviços prestados por pessoa jurídica

3,65%

sobre receitas operacionais¹

PIS/Cofins e ISS possuem como base de cálculo a **receita bruta**³ (incluindo os próprios tributos - cálculo “por dentro”)

Por simplicidade, adotou-se para todas as empresas a **alíquota de PIS/Cofins cumulativa de 3,65%**, observada pelas empresas do Lucro Presumido

Considera-se que tal alíquota **pode ser uma estimativa conservadora da arrecadação para empresas que porventura estariam no Lucro Real** e operariam sobre a incidência não cumulativa

ISS

Municipal

Prestação de serviços

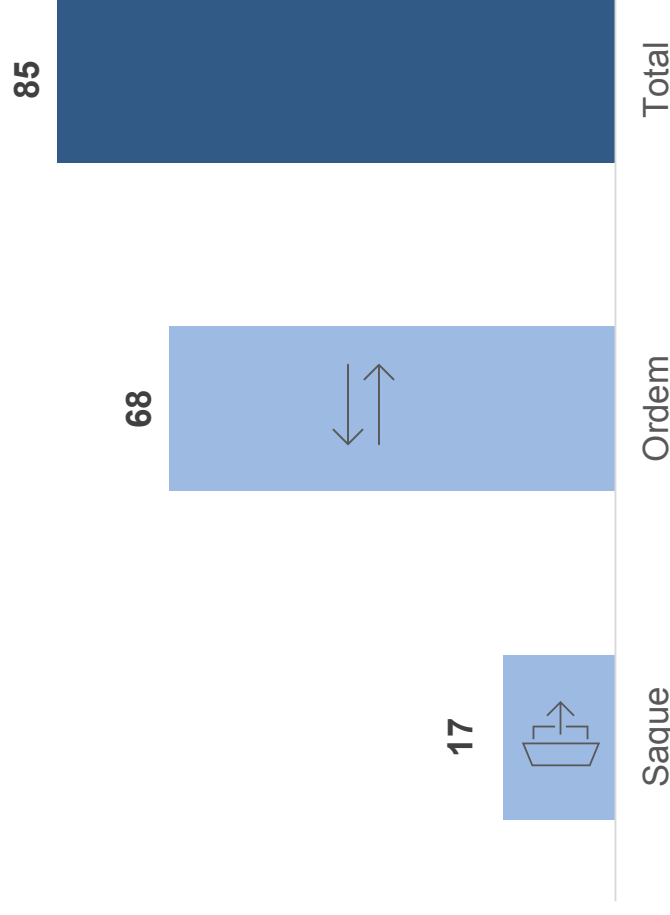
5%

sobre receita com prestação de serviços²



Tributos sobre prestação de serviços representaram **8,65% do faturamento** computado

Estimativa de arrecadação parcial com tributos sobre consumo (PIS/Cofins e ISS), em R\$ milhões 2021



1. Lei nº 10.833/2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/10.833.htm

2. Enquadrada no item 10.01 da Lei Complementar 116/2003, alíquota de 5% válida para o município de São Paulo.

3. Embora as bases de cálculo de ISS e de PIS/Cofins não sejam idênticas, por simplificação as alíquotas dos tributos foram aplicadas sobre o mesmo valor.

TRIBUTOS SOBRE RENDA CORPORATIVA

Tributo

IRPJ

CSLL

Competência

Federal

Federal

Incidência

Renda auferida por pessoas jurídicas

Renda auferida por pessoas jurídicas

Alíquota

25%

sobre lucro tributável¹

9%

sobre lucro tributável²

Observações e premissas

Considerando a grande variabilidade da rentabilidade das empresas no Lucro Real, assume-se, por simplificação, a regra de tributação sobre as empresas do Lucro Presumido; deste modo, IRPJ e CSLL incidiriam sobre **32% da receita bruta**

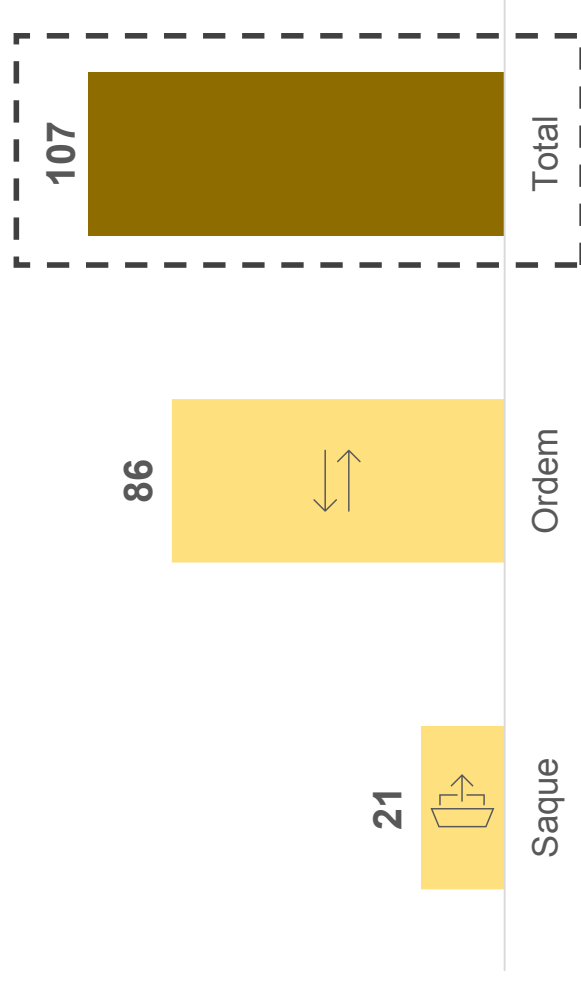


Em 2021 o lucro tributável das exchanges estimado em R\$ 315 mi



Sobre este valor calcula-se a arrecadação de IRPJ e CSLL

Estimativa de arrecadação parcial com tributos sobre a renda corporativa (IRPJ e CSLL), em R\$ milhões (2021)



1. A alíquota base de IRPJ é de 15% para empresas tributadas pelo lucro real ou presumido, contendo um adicional de 10% para lucros superiores a R\$ 20 mil mensais.

2. Alíquota de CSLL de 9% para pessoas jurídicas em geral. Supõe-se que exchanges não se enquadraram na categoria de instituições financeiras, de seguros privados e de capitalização.

TRIBUTOS SOBRE OPERAÇÕES CAMBIAIS

Tributo

IOF

Competência

Federal

Incidência

Operações de crédito

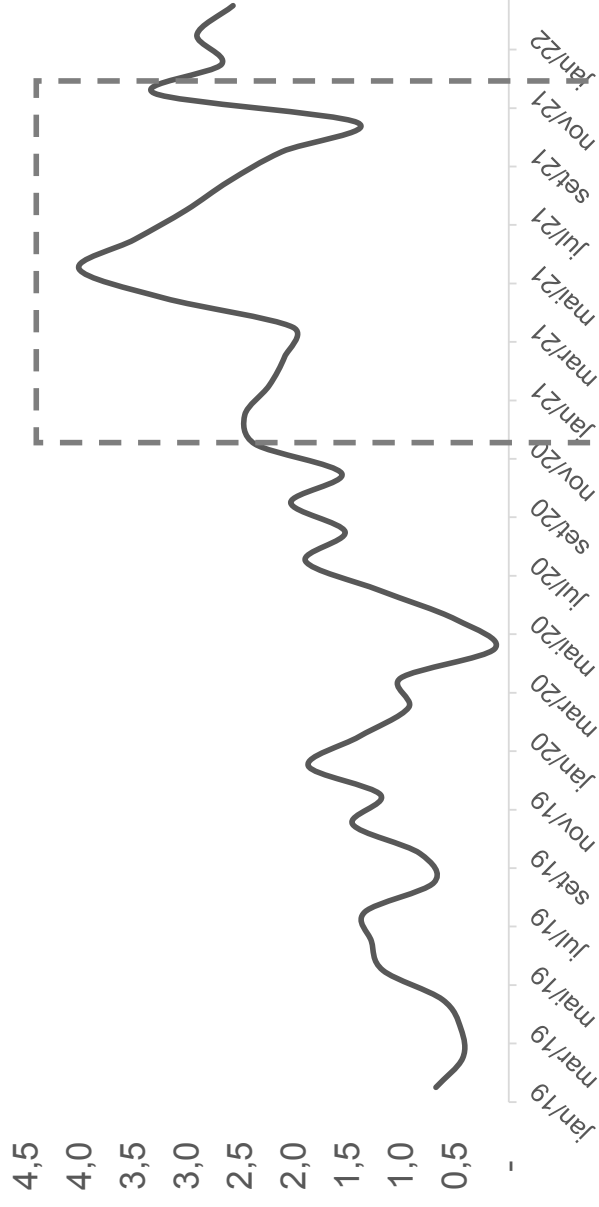
Alíquota

0,38%
sobre operações cambiais¹

Observações e premissas

IOF incide sobre operações cambiais decorrentes de importação de criptoativos. Há possibilidade de arrecadação de IOF na importação de criptoativos na hipótese de celebração de contratos de câmbio

Importações mensais de criptoativos (R\$ bilhões)



Fonte: Banco Central do Brasil. Elaboração: LCA Consultores.



BCB calcula R\$ 32,2 bilhões em importações de criptoativos em 2021

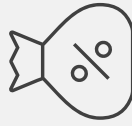


Sobre este valor incide a alíquota de IOF prevista, de modo que o valor arrecadado estimado foi de **R\$ 122 milhões em 2021**

1. Sobre transferências internacionais à terceiros, realizadas em moeda estrangeira, incide alíquota de 0,38% de IOF.

Cenários de conformidade tributária das demais *exchanges* estrangeiras Brasil

- I. Estimativa de receita tributável das *exchanges*
- II. Arrecadação em cenários de internalização de *exchanges*



Estimativa de cenários de sujeição das exchanges estrangeiras e parcialmente nacionalizadas à tributação brasileira para dimensionar o potencial de arrecadação

Formas de sujeição tributária

Exchanges estrangeiras e parcialmente nacionalizadas poderiam estar sujeitas a recolhimentos do sistema tributário brasileiro de duas formas principais:

1. **Criando domicílio fiscal no Brasil** – internalização;
2. **Mantendo suas sedes domiciliadas no exterior e exportando serviços** ao Brasil

Prioriza-se estimativas de internalização neste trabalho, sendo o cenário de importação de serviços, de maior carga tributária para as empresas, apresentado no Anexo VIII

Sujeição tributária, para estes exercícios, não implicaria necessariamente em conformidade a todos os aspectos regulatórios¹

1. Por exemplo, a conformidade a eventuais padrões ambientais estabelecidos na legislação dificilmente poderá ser verificada quando houver importação de serviços.

Exchanges estrangeiras e parcialmente nacionalizadas têm **menores taxas médias** de serviços²:

- Taxa de ordem: **0,43%** para as nacionais/nacionalizadas X **0,20%** para estrangeiras/parcialmente nacionalizadas
- Taxa de saque: **R\$ 5** e **0,40%** para as nacionais/nacionalizadas X **R\$ 3,46** e **0,42%** para estrangeiras/parcialmente nacionalizadas³

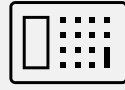


Esse movimento pode levar as taxas de exchanges estrangeiras e parcialmente nacionalizadas mais próximas às cobradas pelas nacionais

- Em tese, pode haver efeitos de migração de consumidores entre os dois tipos de exchanges – por simplicidade, estas não são consideradas nestes cenários



2. Ponderação realizada pelo *market share* de cada exchange. Fonte: CoinTrader monitor. Vide anexo para detalhes. 3. Como as estrangeiras e parcialmente nacionalizadas não recolhem tributos no Brasil, essas taxas não incluem os tributos nacionais.



Foram construídos cenários em que tais exchanges estejam sujeitas as mesmas incidências tributárias que as nacionais e nacionalizadas

Exchanges estrangeiras e parcialmente nacionalizadas cobrariam valores superiores ao que cobram hoje (Cenário A), até no máximo cobrando a taxa das nacionais (Cenário B)

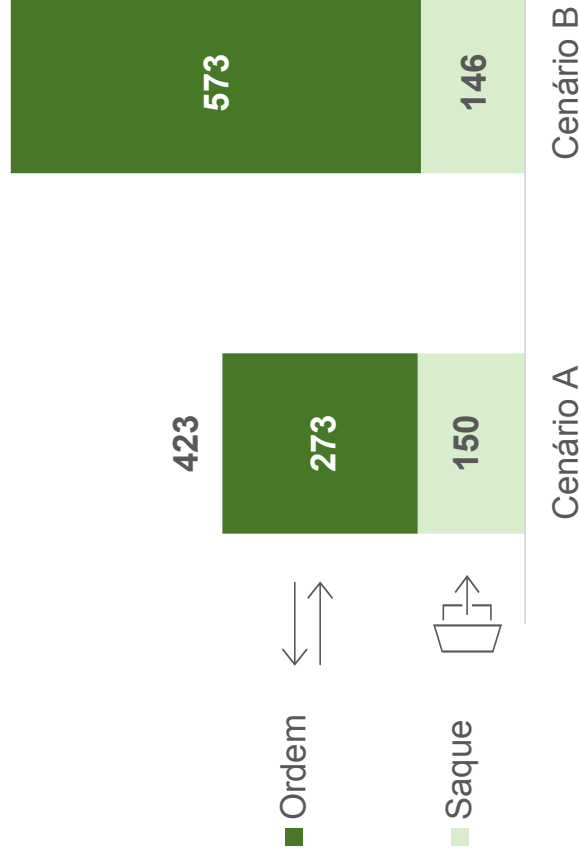
- **Cenário A:** manutenção das taxas atuais¹
- **Cenário B:** taxas das exchanges estrangeiras e parcialmente nacionalizadas iguais às taxas atuais das nacionais e nacionalizadas²

Como as exchanges nacionais e nacionalizadas já pagam tributos, o faturamento calculado com as suas taxas já inclui a valor arrecadado pelo fisco. O mesmo não é verdade para a taxa das demais³.

1. De 0,2% para transações e R\$ 3,46 e 0,42% para saques, acrescidas dos tributos sobre transações internas. 2. Taxa de 0,43% para transação e R\$ 5 e 0,40% para saques, já incluindo a incidência de PIS/Cofins e ISS. 3. Esse fato tem implicações sobre o cálculo se arrecadação, uma vez que a base de incidência é diferente.

Estimativa de faturamento das exchanges estrangeiras e parcialmente nacionalizadas nos cenários de internalização, em R\$ milhões (2021)

719



Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinify.
Elaboração LCA Consultores.



Exchanges passariam a possuir domicílio fiscal no Brasil (seriam internalizadas) e passariam a contribuir da mesma forma que as exchanges nacionais e nacionalizadas

Premissas de tributos sobre prestação de serviços e renda são **análogos à sessão anterior**

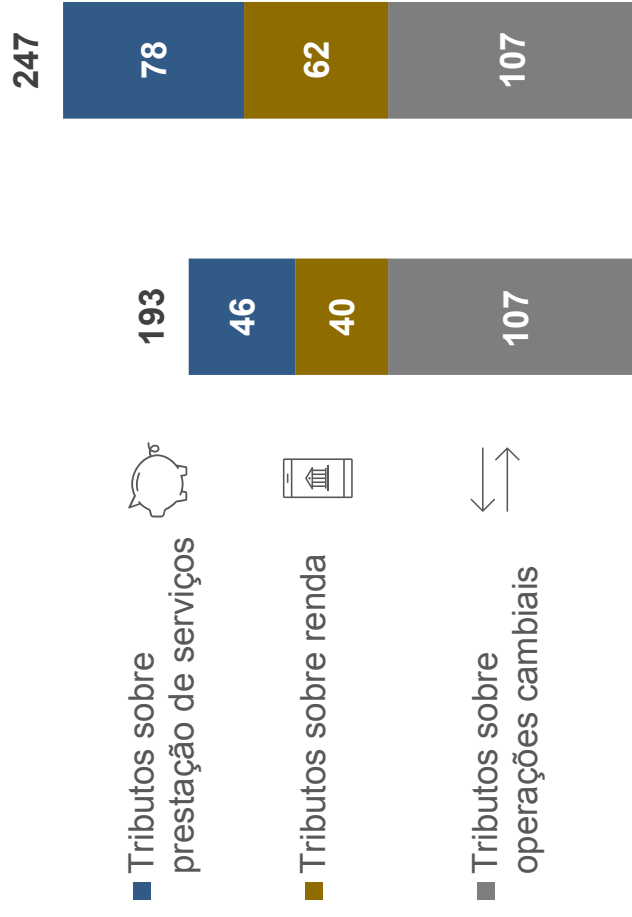
Para o IOF, adicional de importações de criptoativos

- Premissa: *share* de importações de tais *exchanges* é igual ao do mercado de transações: **importação de R\$ 28,2 bilhões em criptoativos para as exchanges estrangeiras e parcialmente nacionalizadas** em 2021, além dos R\$ 32,2 bilhões identificados pelo BCB
- Internalização obrigaria *exchanges* a celebrar contratos de câmbio, forma de trocar os reais faturados no mercado interno para as moedas estrangeiras utilizadas em suas sedes
- Arrecadação com IOF não difere entre os cenários uma vez que não depende das taxas cobradas pelas *exchanges*



Se a regulação englobasse exchanges estrangeiras e parcialmente nacionalizadas, haveria potencial de aumento de até 79% na arrecadação, equivalente a R\$ 247 milhões em 2021

Estimativa de arrecadação nos cenários de internalização das demais exchanges, em R\$ milhões (2021)



Cenário A Cenário B

Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcoinity e BCB.
Elaboração LCA Consultores.

Atuais contribuintes + internalização de estrangeiras e parcialmente nacionalizadas (2021):

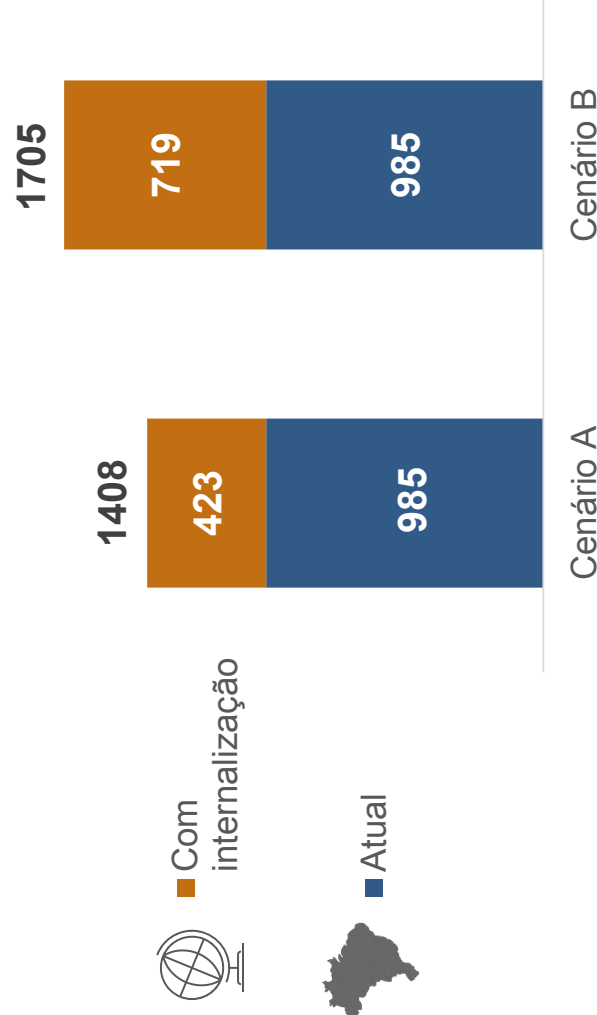


Faturamento das exchanges entre R\$ 1,4 e R\$ 1,7 bilhões



Exchanges têm potencial de contribuir para o fisco com mais de meio bilhão de reais em ambos cenários

Estimativa de faturamento total nos dois cenários apresentados, em R\$ milhões (2021)



Nota: O faturamento calculado pelo cenário A também serve de base para as estimativas de tributação de importação de serviços. Fonte: Diversas. Elaboração LCA Consultores.

Estimativa de arrecadação total nos dois cenários apresentados, em milhões (2021)

Cenário	Exchange	Prestação de serviços	Renda	Operações cambiais	Total
Cenário A	Atuais contribuintes	R\$ 85	R\$ 107	R\$ 122	R\$ 314
	Com internalização	R\$ 40	R\$ 46	R\$ 107	R\$ 193
	Total	R\$ 125	R\$ 153	R\$ 229	R\$ 507
Cenário B	Atuais contribuintes	R\$ 85	R\$ 107	R\$ 122	R\$ 314
	Com internalização	R\$ 62	R\$ 78	R\$ 107	R\$ 247
	Total	R\$ 147	R\$ 185	R\$ 229	R\$ 561

Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity.
Elaboração LCA Consultores.

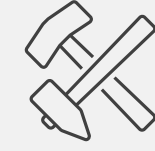
Anexos

- I. Demais conceitos da criptoeconomia
- II. Divisão das *exchanges* e cálculo de taxas
- III. Bases de dados e conformidade com a RFB
- IV. Panorama regulatório internacional e em jurisdições selecionadas
- V. Segmentação regulatória de ativos financeiros no Brasil
- VI. Pedidos de dados via Lei de Acesso a Informação (LAI)
- VII. Exemplificação da metodologia – *Exchange* fictícia
- VIII. Cenário de importação de serviços



Blockchain

- Sistema de **armazenamento de informações**, cuja principal característica é o armazenamento periódico em lotes (**blocos**) interligados em ordem cronológica
- Vantagem advém de ser um processo **inteiramente descentralizado**, independente de um intermediador central, capaz de garantir transparência e honestidade
- Dados são praticamente imutáveis - mudanças afetam todo o sistema e devem ser aceitas pelos participantes da rede
- **Blockchains** podem ser públicas (geral) ou privadas (alguma entidade central como empresas ou governos, que regulam o acesso a dados e as informações)



Mineração de criptoativos é recompensa ao processo de autenticação de transações realizadas no *blockchain*, que pode ser feita de duas formas:



Proof-of-Work (PoW)

Sistema de mineração utilizado pela maioria dos criptoativos em que computadores precisam resolver problemas matemáticos complexos, com **elevados gastos energéticos**



Proof-of-Stake (PoS)

Validadores ganham uma recompensa à autenticação de uma transação de acordo com o nº de criptoativos “apostados”

Armazenamento

- Criptoativos são armazenados em carteiras na *blockchain*; sistema descentralizado permite segurança aos detentores das chaves de cada carteira
- Ativos podem ser armazenados em *hot wallets* - carteiras online - ou *cold wallets* (*hardwares* como *pen drives*)



₿ Mineração de Bitcoin

- ▶ O menor custo da energia da China a torna, historicamente, o principal polo de mineração de bitcoin, até a **proibição estabelecida em mai/2021**
- ▶ Parte dos mineradores chineses voltaram a operar, em parte devido ao uso de VPNs (rede privada que permite alteração de localização), de forma que o país é o segundo maior na produção de mineração de BTC no mundo, apenas atrás dos EUA

ANEXO II - DIVISÃO DAS EXCHANGES E CÁLCULO DE TAXAS

Exchanges utilizadas na análise, taxas de maio de 2022

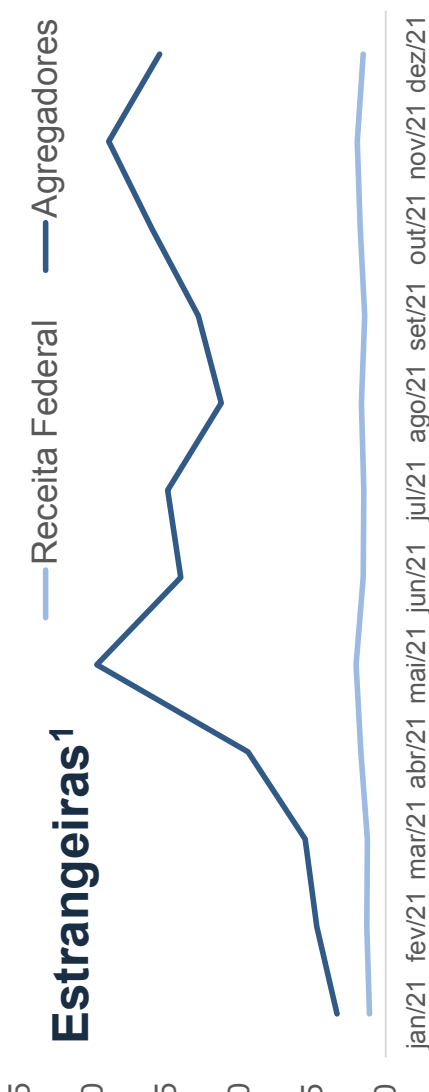
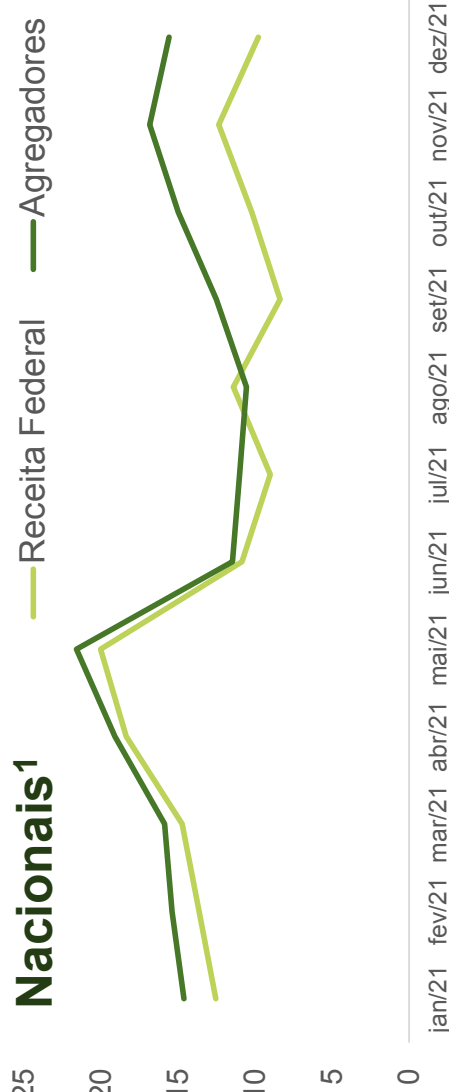
Exchange	Classificação	Share 2021	Share 2020	Taxa de ordem	Fixo Saque	Variável Saque	CNAE 6619-3/99
Binance	Estrangeira	29,8%	1,3%	0,10%	R\$ 2,60	0,00%	Não registrada
BitPreço	Nacional	13,4%	12,0%	0,20%	R\$ 4,90	0,20%	Atividade secundária
MercadoBitcoin	Nacional	13,2%	21,5%	0,70%	R\$ -	0,00%	Atividade secundária
NovaDAX	Nacionalizada	12,3%	15,1%	0,50%	R\$ 8,90	1,50%	Atividade principal
BitcoinToYou	Parcialmente Nacionalizada	8,7%	10,2%	0,60%	R\$ 9,99	1,89%	Não registrada
Foxbit	Nacional	3,8%	5,8%	0,50%	R\$ -	0,00%	Não registrada
FTX	Estrangeira	2,8%	0,6%	0,07%	R\$ 10,00	0,30%	Não registrada
Coinext	Nacional	2,5%	4,3%	0,50%	R\$ 8,99	0,19%	Atividade principal
BitcoinTrade	Nacionalizada	2,4%	6,4%	0,50%	R\$ 4,90	0,00%	Atividade principal
PagCripto OTC	Nacional	2,3%	0,7%	0,25%	R\$ 10,00	0,00%	Atividade principal
UpCâmbio	Nacional	1,5%	0,9%	0,25%	R\$ 10,00	0,35%	Não registrada
YouBtrade	Nacional	1,1%	0,6%	0,30%	R\$ 9,90	0,00%	Atividade principal
Bisoint	Nacional	0,9%	0,9%	0,00%	R\$ 14,90	0,00%	Atividade secundária
Brasil Bitcoin	Nacional	0,8%	1,7%	0,50%	R\$ 5,00	0,50%	Não registrada
Makes Exchange	Nacional	0,7%	1,5%	0,00%	R\$ -	0,00%	Atividade secundária
Demais Nacionais	Nacional	3,0%	16,4%	-	-	-	-
Demais Parc. Nacionalizadas	Parcialmente Nacionalizada	0,8%	0,1%	-	-	-	-

Nota: Cálculo das taxas médias de nacionais e estrangeiras foi realizado através de uma média ponderada pelo share das exchanges, em que foram consideradas todas as empresas com dados disponíveis na data de coleta. A tabela apresenta apenas as exchanges com share maior que 0,5%, o restante das empresas foi agregada nas linhas "Outras".

Classificação: Existem empresas com CNPJ no Brasil e quadro societário composto apenas por pessoas jurídicas situadas no exterior, no entanto elas foram classificadas como parcialmente nacionalizadas por possuir empresa filiada no exterior (exemplo: BitcoinToYou e BitcoinToYou Internacional). As empresas nacionalizadas foram definidas por participarem de Holdings no exterior (NovaDAX – China e BitcoinTrade/Ripio – Ilhas Cayman).

Fonte: CoinTrade Monitor, em maio de 2022. Elaboração LCA Consultores.

volução do mercado de transações de criptoativos em *exchanges* nacionais e estrangeiras, por base de dados



Nota: 1. Para essa comparação considerou-se como nacionais também as nacionalizadas, e como estrangeiras também as parcialmente nacionalizadas. 2. Informações do CoinTradeMonitor são originalmente restritas ao BTC, entretanto o mercado é corrigido com através da informação de proporção do BTC no mercado nacional, disponibilizado pelo LiveCoins. Fontes: Coin Trade Monitor, Livecoins e Receita Federal do Brasil. Elaboração LCA Consultores.



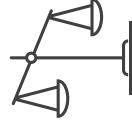
Bases de dados

RFB: Dados de transações mensais com criptoativos declarados à Receita. O órgão utiliza uma classificação própria para *exchanges* nacionais e estrangeiras¹.

- Observam algumas operações fora do livro aberto²

Agregadores: Dados do *CoinTrader Monitor* e do *LiveCoins*, em valores transacionados em *exchanges*³. A segmentação entre *exchanges* é própria deste trabalho.

- São sites que computam todas as operações feitas em livro aberto, não observam transações realizadas por OTCs



Devido a obrigatoriedade da IN 1.888 em reportar transações, dados para *exchanges* nacionais⁴ são **coerentes** entre a RFB e os agregadores. Entretanto, a RFB observa apenas **parte diminuta** das transações feitas em estrangeiras⁴, uma vez que elas **não se conformam** a regulação

Neste trabalho, opta-se pelo uso das informações dos agregadores por conterem dados abrangentes de *exchanges* estrangeiras⁴

1. A RFB informou a LCA Consultores que segmenta as *exchanges* de acordo com domicílio fiscal, fator que também norteou a classificação deste trabalho. 2. Realizadas em OTCs e parte das operações P2P (~16% do total declarado) 3. Segundo a fonte: “Esses dados são coletados diretamente das API disponibilizadas pelas próprias *exchanges*. Considera-se que as informações oferecidas através destes canais são **DECLARAÇÕES** e que não foram submetidas a auditoria externa”. 4. Para essa comparação considerou-se como nacionais também as nacionalizadas, e como estrangeiras também as parcialmente nacionalizadas.



Segundo relatório do Congresso Americano (130 países avaliados)

- Em jun/2018, **somente 33 países** apresentavam algum tipo de legislação para regulação de criptoativos (tributação e/ou prevenção de lavagem de dinheiro e financiamento de terrorismo);
- Em nov/2021, **103 países (~77%)** apresentam alguma destas legislações, geralmente ambas, com forte influência da extensão da legislação europeia implementada em 2020;

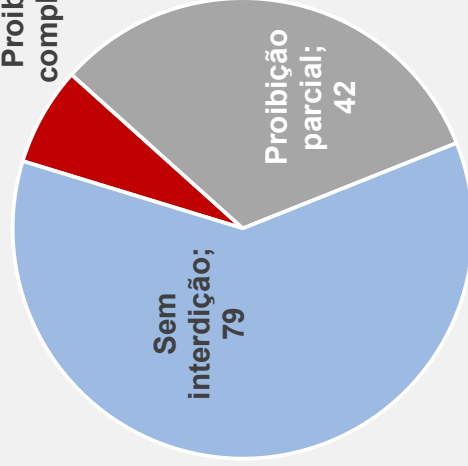


Proibição de criptoativos pelo mundo (2021)

Proibição completa; 9

- Criptoativos são inteiramente banidos em **9 países, incluindo a China** (exceto yuan digital, CBDC em desenvolvimento)

- **42 países apresentam proibições parciais** em criptoativos, como impedir uso destes como meio de pagamento (Turquia) ou interditar operação de *exchanges* e aquisição por inst. financeiras (Bolívia)



Japão



- **Legislação avançada** reconhece criptoativos como propriedade legal e como **meio de pagamento**
- *Exchanges* devem ser registradas pela autoridade de serviços financeiros



Suíça



- **Polo de desenvolvimento de criptoativos** com legislação avançada para ICOs
- Criptoativos são considerados ativos intangíveis, **exceto para exchanges, para os quais criptoativos são inventário**



Estônia



- Referência no uso de *blockchain* para a **digitalização da burocracia**
- *Exchanges* devem ser registradas pela autoridade de serviços financeiros



Valores Mobiliários

Lei nº 6.385/1976

Títulos ou contratos de investimento ofertados publicamente, que gerem direito de participação dos quais os rendimentos advêm de esforços do empreendedor



Principal Legislação



Definição



Principais agentes do mercado



Órgão Regulador



Atribuições do Órgão



Moedas Eletrônicas

Lei nº 12.865/2013

Recursos armazenados em dispositivo ou **sistema eletrônico** que permitem ao usuário efetuar a transação de pagamento

Representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou como investimento

Instituições de **Pagamento** e Instituidores de **Arranjos de Pagamento**

Prestadoras de serviços de ativos virtuais

Banco Central (a partir de diretrizes do CMN)

Não estabelecido. A ser definido pelo Poder Executivo Federal

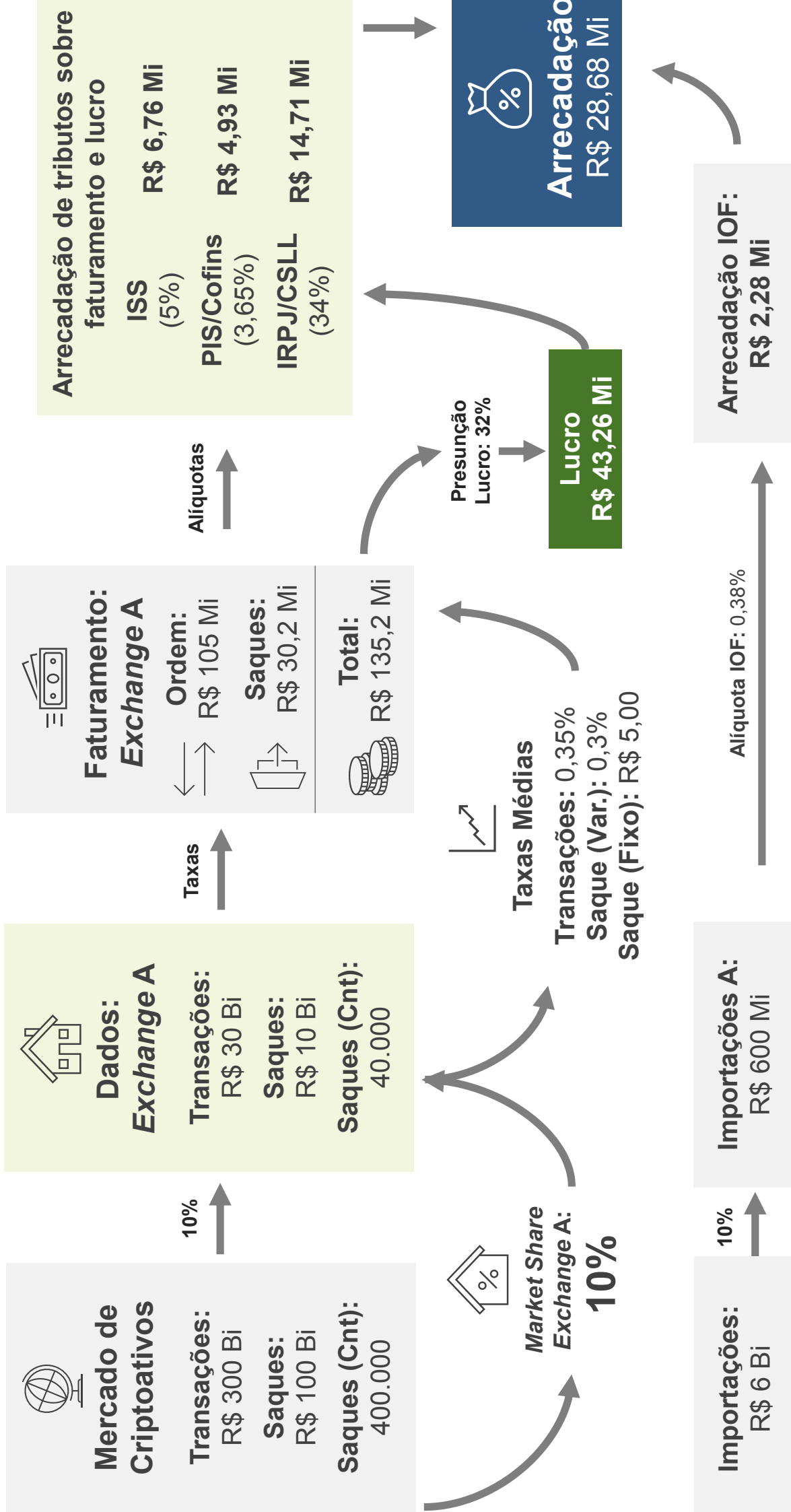
Disciplinar, fiscalizar e limitar o objeto social de instituições de pagamento; assegurar solidez e eficiência de arranjos de pagamento

Supervisionar prestadoras de serviços. Cancelar ou suspender autorizações, em caso de descumprimento das normas do PL

Pedidos de acesso a informação realizados pela LCA Consultores

Data de Resposta	Órgão	Resumo	Demanda	Resposta
25/06/2022	BCB	Custódia de Criptoativos	Solicito melhor entendimento sobre quais tipos de informação o Banco Central possui sobre a custódia de criptoativos. Informações como esta enunciada pelo presidente do BC, citada abaixo, derivam de contratos de câmbio, importação de criptoativos, <i>market-makers</i> , ou de informações da Receita Federal? Quais bases de dados o BC dispõe sobre o assunto? Estas são públicas? "O presidente do BC destacou ainda que os criptoativos cresceram mais no Brasil como investimento do que como meio de pagamento e destacou que há concentração de custódia desses ativos. "83% dos ativos em cripto estão em quatro custodiantes", afirmou."	O Banco Central não possui informação oficial sobre custódia de criptoativos. O dado mencionado pelo presidente provém de informação preliminar sobre o assunto.
02/06/2022	BCB	Importação e Exportação de Criptoativos	Solicito, por gentileza, as séries mensais completas de importação e exportação de criptoativos, em todos os anos em que estas estiverem disponíveis. Também solicito informações adicionais de como é feita a estimativa destes. Os contratos de câmbio de criptoativos são estimados através de informações de <i>exchanges</i> ?	A fonte das exportações e das importações de criptoativos é o contrato de câmbio, que pode ser realizado por qualquer residente (pessoa física ou pessoa jurídica, exchange ou não). Entretanto, operadores de grande porte têm predominado como contraparte residente desses contratos de câmbio. A identificação da operação vinculada ao criptoativo é realizada por meio de um código cambial e um campo texto em que a parte residente do contrato de câmbio presta essa informação. Cabe lembrar que, por definição, importação e exportação referem-se à mudança de propriedade (no caso do criptoativo) entre residente e não residente. Portanto, compras/vendas de criptoativos entre residentes, diretamente no mercado doméstico, não fazem parte do escopo dessas séries.
22/07/2022	RFB	Criptoativos – PJ por CNAE	Solicito as informações de valor declarado em criptoativos por PJs, segregado por uso de <i>exchanges</i> no exterior e sem uso de <i>exchanges</i> , no maior nível de desagregação por CNAE possível. Solicito esta informação para todos os meses em que esta estiver disponível.	Em atenção à sua solicitação, informamos que dados abertos sobre as operações de criptoativos estão disponíveis no site da Receita Federal do Brasil. Solicitações contempladas pelos dados já publicados deixam de ser atendidas com base no inc. II do art. 13 do Decreto nº 7.724, de 2012.
22/07/2022	RFB	Criptoativos – Exchanges nacionais e exchanges no exterior	Solicito o modo no qual a Receita Federal do Brasil diferencia <i>exchanges</i> nacionais e <i>exchanges</i> no exterior, e se esta classificação sofreu alguma alteração desde que os dados de declarações em criptoativos passaram a ser obtidos.	Em atenção à sua solicitação, informamos que a classificação é feita com base no domicílio tributário da <i>exchange</i> . Não houve mudança nessa orientação. As domiciliadas no país estão obrigadas a prestar informações à Receita Federal. No caso de operações realizadas fora de <i>exchange</i> ou em <i>exchange</i> no exterior, as informações devem ser prestadas pela pessoa que realizar a operação com criptoativo.
19/08/2022	RFB	Criptoativos - Pessoas Físicas Declarantes	Solicito informações sobre o perfil das pessoas físicas declarantes de criptoativos no menor nível de agregação possível. O relatório nº 3 dos dados abertos da RFB apresenta o nº de operações e valor de operação por sexo: solicito estas informações também estratificadas por idade, nível de renda, ocupação dos indivíduos e unidade federativa de domicílio. Solicito esta informação para todos os anos em que ela estiver disponível.	Em atenção à sua solicitação, informamos que os dados estão disponíveis apenas no nível de agregação divulgado no relatório 3 citado pelo solicitante. O fornecimento da informação na forma solicitada envolve trabalhos adicionais de análise, interpretação ou consolidação de dados.

ANEXO VII - EXEMPLIFICAÇÃO DA METODOLOGIA – EXCHANGE FICTÍCIA COM 10% DE MARKET-SHARE



Serviços de exchanges estrangeiras e parcialmente nacionalizadas passam a ser tributados como **serviços importados**, com os tributos incidindo sobre faturamento líquido do cenário A



- Optou-se por incidir sobre o faturamento com as taxas atuais das exchanges estrangeiras e parcialmente nacionalizadas (*idem* cenário A) uma vez que as taxas das exchanges nacionais e das nacionalizadas já incluem os tributos pagos internamente
- Geralmente incidem **seis tributos sobre serviços importados no Brasil**, apresentados na Tabela abaixo

Tributos sobre importação de serviços

Tributo	Base de cálculo	Alíquota
IRRF ¹	Valor do serviço ² + IRRF + CIDE + ISS	15% (geral, válida para serviços técnicos); 25% (não técnicos e "paraísos fiscais")
CIDE-Remessas	Idem a IRRF	10% (apenas para serviços técnicos)
ISS	Idem a IRRF	5% (a depender do município) ³
PIS/COFINS-Importação	Idem a IRRF + o próprio PIS/COFINS-Importação ⁴	9,25%
IOF	Valor do serviço, acrescido da CIDE-Remessas	0,38%

Notas: 1. Regime de incidência do IRRF pode provocar distorções competitivas uma vez que os serviços importados já são tributados em seu país de origem. Para evitar essa situação, é comum os parceiros celebrarem acordos bilaterais (ADTs). 2. Valor líquido dos tributos brasileiros recebido pelo prestador estrangeiro. 3. Premissa para esse exercício é de alíquota de 5% (cidade de São Paulo). 4. Segundo a IN RFB n. 1.911/2019, o PIS/COFINS-Importação para serviços deve ser calculado segundo a seguinte fórmula: $a * V * z$, onde: a é a alíquota; V é o valor da contratação, ou seja, valor recebido pelo prestador estrangeiro somado aos tributos retidos na fonte (IRRF, CIDE-Remessas e ISS); e z = $(1 + \text{alíquota do ISS}) / (1 - \text{alíquota do PIS/COFINS})$.

Elaboração: LCA Consultores

Considera-se o serviço prestado pelas exchanges como **técnico**, com incidência de CIDE-Remessas

- **Premissa tem pouco impacto sobre os resultados**, uma vez que serviços técnicos estão sujeitos a uma alíquota menor de IRRF na mesma proporção do CIDE-Remessas¹

Entende-se que não há aproveitamento de possíveis créditos do PIS-Cofins Importação, sendo tais serviços de intermediação em geral destinados ao consumidor final (pessoa física)

1. O único impacto dessa definição para o valor arrecadado é um aumento diminuto da base de cálculo do IOF, composta pela arrecadação do CIDE-Remessas.

Quando comparados aos resultados dos cenários de internalização, destaca-se:

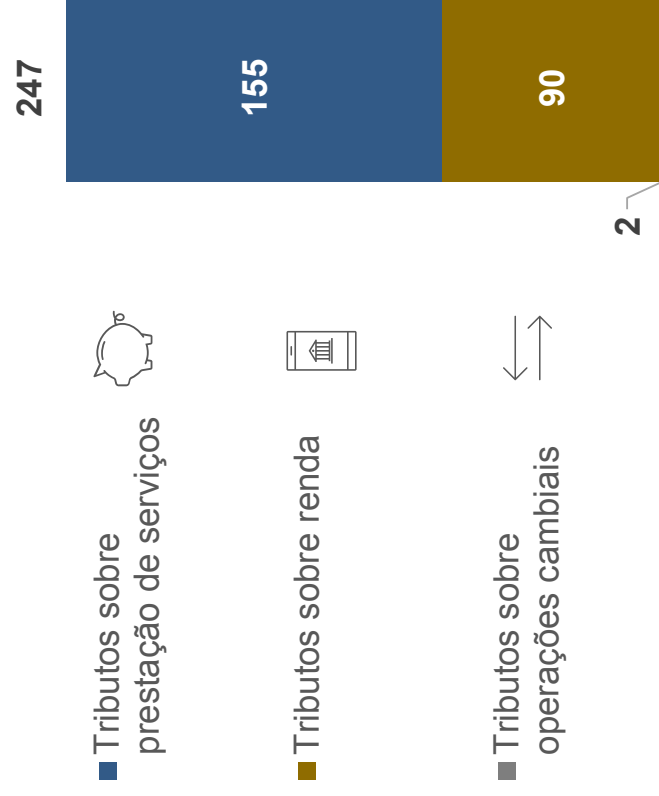
- **Maior arrecadação com tributos sobre a prestação de serviços**, devido a maior alíquota de PIS/Cofins e a incidência de CIDE-Remessas
- **Maior arrecadação de IR**, pela alíquota de 15%, frente aos 10,88%, mesmo desconsiderando possível tributação de renda corporativa no país sede
- **Menor arrecadação de IOF** pela diferença na base de incidência, agora relativa ao valor do serviço – nos cenários de internalização tributo incidia sobre o valor total dos criptoativos nos contratos cambiais

! Conformidade via importação de serviços pode ser desfavorável

Aponta-se que o processo de conformidade por exportação de serviços não seria escolhido pelas *exchanges* estrangeiras e parcialmente nacionalizadas por implicar, em tese, em maior recolhimento tributário e taxas mais altas ao consumidor

- Embora a valor arrecadado seja igual ao do cenário B de internalização, naquele cenário o faturamento das empresas é significativamente superior (uso de taxas análogas às nacionais e nacionalizadas)

Estimativa de arrecadação nos cenários de importação de serviços das *exchanges* estrangeiras e parcialmente nacionalizadas, em R\$ milhões (2021)



Importação de serviços

*Nota: Considera-se o CIDE-Remessas como tributo sobre prestação de serviços.
Fonte: Coin Trader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcolnity e BCB.
Elaboração LCA Consultores.*



www.lcaconsultores.com.br



Panorama setorial da criptoeconomia no Brasil

Novembro de 2022

Sumário

Introdução	1
2. Contextualização sobre os criptoativos e a criptoeconomia	3
2.1 Classificação de criptoativos	5
2.1.1 Payment <i>Tokens</i> (ou <i>tokens</i> de pagamento)	7
2.1.2 Outros <i>Tokens</i>	9
2.2 Evolução do mercado mundial de criptoativos	12
2.3 <i>Exchanges</i> de criptoativos	15
3. Criptoeconomia e <i>exchanges</i> no Brasil	18
3.1 Indicadores de evolução do mercado e participação por criptoativos	18
3.2 Importações	22
3.3 Dimensionamento de mercado	23
3.3.1 Classificação das <i>exchanges</i> no Brasil	23
3.3.2 Participação de mercado das <i>exchanges</i>	25
3.3.3 Dimensionamento das transações	27
4. Desafios regulatórios	30
4.1 Panorama regulatório internacional	32
4.1.1 Estados Unidos	32
4.1.2 União Europeia	34
4.2 Regulação no Brasil	36
4.2.1 Histórico regulatório	37
4.2.2 Projeto de lei em discussão no Brasil: PL 4.401/2021	39
5. Tributação de <i>exchanges</i> de criptoativos no Brasil	41
5.1 Estimativa da tributação atual	44
5.1.1 Estimativa do faturamento tributável das <i>exchanges</i> nacionais e nacionalizadas	45
5.1.2 Cálculo da arrecadação tributária	48
5.2 Estimativa da tributação potencial das <i>demais exchanges</i>	51
Conclusão	59
Anexos	61
Anexo 1: Divisão das <i>exchanges</i> e cálculo de taxas	61
Anexo 2: Pedidos de dados via Lei de Acesso à Informação (LAI)	62
Anexo 3: Exemplificação da metodologia – <i>exchange</i> fictícia	64
Anexo 4: Comparação dados agregadores e RFB	64

Introdução

Desde 2008, ano do surgimento do Bitcoin, instituições governamentais por todo o mundo observam a revolução dos criptoativos e o surgimento da criptoeconomia. Suas características disruptivas – confrontando concepções tradicionais de moeda, ativo e posse, dentre outras – bem como as novas formas de geração de valor relacionadas aos criptoativos provocam amplas discussões quanto a como regular e tributar os diversos produtos e serviços que os envolvem.

Está longe de haver consenso internacional quanto à definição de criptoativos, sua natureza ou atribuições de responsabilidade entre agências regulatórias. Embora muitos países proíbam, ainda que parcialmente, o uso de criptoativos, a maior parte das jurisdições apresentaram avanços quanto à proposição de arcabouços regulatórios mais abrangentes. Exemplos disso são a proposta MiCA (*Markets in Crypto-Assets*)¹ do Parlamento Europeu e a *Lummis-Gillibrand Crypto Bill*², em discussão no Congresso americano.

No Brasil, a Instrução Normativa (IN) 1.888/2019³ da Receita Federal do Brasil (RFB) constituiu um importante avanço na regulação de transações de criptoativos. Esta versa principalmente sobre tributação de renda e ganhos de capital nestas operações, e instituiu a obrigatoriedade de *exchanges* prestarem informações ao fisco sobre movimentação de valores de seus clientes.

O Congresso Nacional debate atualmente um marco regulatório mais abrangente para a criptoeconomia, como proposto no Projeto de Lei (PL) 4.401/2021⁴, tratando das questões relacionadas a autoridade de cada órgão para regulação, fiscalização e tributação de transações com ativos virtuais através de *exchanges*, segurança do patrimônio dos usuários e coibição de práticas ilegais, bem como obrigatoriedade de autorização prévia para a prestação de serviços ligados a ativos virtuais.

¹ Disponível em <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593>. Acesso em 08/09/2022.

² Disponível em <https://www.congress.gov/bill/117th-congress/senate-bill/4356/text>. Acesso em 08/09/2022.

³ Disponível em <http://normas.receita.fazenda.gov.br/sijut2consulta/link.action?idAto=100592>. Acesso em 02/09/2022.

⁴ Texto inicial do PL disponível em <https://www25.senado.leg.br/web/atividade/materias/-/materia/151264>. Acesso em 02/09/2022.

Nesse contexto, a ABCripto solicitou à LCA Consultores a elaboração de um estudo com objetivo de apresentar um panorama setorial da criptoeconomia no Brasil, em conjunto com a discussão do estado regulatório, nacional e internacional. Adicionalmente, o trabalho apresenta também estimativa de arrecadação potencial de transações com criptoativos no Brasil, bem como cenários alternativos em que as operações de *exchanges* atualmente não totalmente domiciliadas no Brasil passem a fazer recolhimentos dos tributos incidentes sobre operações realizadas no mercado doméstico.

Com estes objetivos, o trabalho divide-se em seis seções, incluindo esta Introdução e a Conclusão. Inicialmente, na Seção 2, discutem-se os principais conceitos envolvendo criptoativos e a criptoeconomia, bem como as principais aplicações existentes e em desenvolvimento da tecnologia e a operação das *exchanges*. Na sequência, na Seção 3, apresenta-se um panorama setorial da criptoeconomia no Brasil, com levantamento de informações públicas acerca dos usuários, empregos, balança comercial e volume de transações com criptoativos, entre outros. A Seção 4 aborda os principais desafios regulatórios do setor, bem como as principais propostas regulatórias em discussão nos EUA, União Europeia e Brasil. A Seção 5 apresenta as estimativas de arrecadação atual, passando rapidamente pela experiência internacional sobre tributação de criptoativos, e incluindo cenários de conformidade ao fisco brasileiro das demais *exchanges*. Por fim, a seção de Conclusão encerra este parecer.

2. Contextualização sobre os criptoativos e a criptoeconomia

Em 2008, o artigo “*Bitcoin: A Peer-to-Peer Electronic Cash System*”,⁵ de autoria atribuída a Satoshi Nakamoto, institui o método para a implementação e o desenvolvimento da rede de transações de Bitcoin, com objetivo de permitir transferências diretas, descentralizadas e anônimas.

A rede Bitcoin, que utiliza essa moeda digital como meio de troca, foi a introdução da tecnologia blockchain, uma aplicação da *Digital Ledger Technology* – DLT (registro eletrônico distribuído). DLTs são bancos de dados geridos por diversos participantes, de forma transparente e não centralizada; o blockchain, em específico, é um sistema de armazenamento de informações cuja principal característica é a retenção periódica em lotes (blocos) interligados em ordem cronológica. A principal vantagem da tecnologia advém desse processo ser inteiramente descentralizado, independente de um intermediador central⁶. Os dados inseridos na blockchain são praticamente imutáveis: mudanças afetariam todo o histórico do sistema e devem ser aceitas por todos os participantes da rede.

Desse modo, o Bitcoin é sistematicamente considerado o primeiro criptoativo, apesar da ausência de uma definição amplamente reconhecida e consensual sobre o que são criptoativos. Para os propósitos deste trabalho, a definição do Fundo Monetário Internacional (FMI) é favorecida:

*Criptoativos são representações digitais de valor, criados com utilização de criptografia, a partir de tecnologia de registro eletrônico distribuído*⁷.

O processo de autenticação de transações e mineração de criptoativos – isto é, como novos criptoativos são criados e a quem estes se destinam – é descrito no Box 1 a seguir. Criptoativos são armazenados em carteiras, que se configuram como meios de armazenar as “chaves” (endereços) públicas e privadas. De posse de uma chave

⁵ Disponível em <https://bitcoin.org/bitcoin.pdf>. Acesso em 09/09/2022.

⁶ Usualmente as blockchains são públicas, permitindo a visualização e autenticação das informações por qualquer indivíduo. Existem também blockchains privadas, em que alguma entidade central - como uma empresa ou um governo – regulam o acesso às informações contidas na corrente.

⁷ Fonte: Sexta edição do Manual de Balanço de Pagamentos e Posição de Investimento internacional (BPM6) do FMI.

privada, pode-se fazer uma transação na blockchain, transferindo o ativo para uma carteira vinculada a uma chave pública. Ao armazenamento de criptoativos em carteiras pode ocorrer em *hot wallets* – carteiras online – ou *cold wallets* (*hardwares* como *pen drives*).

Box 1: Mineração e autenticação de criptoativos – histórico e regulação

O processo de mineração de criptoativos é a recompensa à autenticação de transações realizadas no blockchain. Essa dinâmica pode ser dividida em duas formas abrangentes:

Proof-of-Work (PoW): Sistema de mineração utilizado pela maioria dos criptoativos, nele computadores precisam resolver problemas matemáticos complexos, com elevados gastos energéticos. Existe grande preocupação dos reguladores internacionais quanto aos crescentes dispêndios na mineração de criptoativos, em especial o Bitcoin; o sistema de mineração não é considerado escalável, de modo que o gasto de energia para o processo aumenta mais que proporcionalmente com o número de módulos realizando-o.

Proof-of-Stake (PoS): Validadores ganham recompensa à autenticação de uma transação de acordo com a quantidade de criptoativos “apostados”. Esse sistema é menos difundido e testado, mas possui em tese maior escalabilidade, devido ao gasto energético diminuto. Em especial, a rede Ethereum busca transitar de um sistema PoW para o PoS, com expectativa de reduzir os gastos energéticos em cerca de 99,95%⁸.

Mineração de Bitcoin pelo mundo

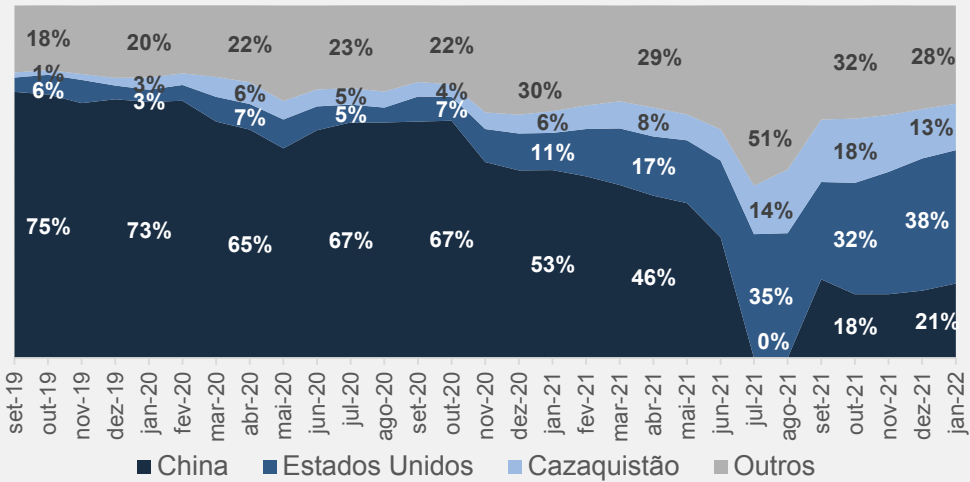
A Universidade de Cambridge⁹ estima que atualmente a mineração do Bitcoin demandou em 2021 aproximadamente 105 TWh, consumo similar ao de países como Holanda e Argentina.

O menor custo da energia da China a tornou, historicamente, o principal polo de mineração de Bitcoin, até a proibição da atividade em maio de 2021. Parte dos mineradores chineses voltou a operar, em parte devido ao uso de VPNs (rede privada que permite alteração de localização), de forma que no período subsequente o país é o segundo maior na mineração de Bitcoin no mundo, apenas atrás dos EUA, conforme exposto no Gráfico 1.

⁸ Fonte: <https://ethereum.org/en/upgrades/merge/>. Acesso em 06/09/2022.

⁹ Fonte: <https://ccaf.io/cbeci/index>. Acesso em: 01/06/2022.

Gráfico 1: Distribuição espacial da mineração de Bitcoin, por país, de setembro de 2019 a janeiro de 2022



Fonte: CCAF. Elaboração: LCA Consultores.

2.1 Classificação de criptoativos

Criptoativos também podem ser denominados, em um conceito mais amplo, como *tokens*, isto é:

Sequência de caracteres que constitui uma representação criptográfica de um conjunto de direitos, que pode ser utilizada dentro de um contexto específico. Não são originalmente monetários.¹⁰

Tokens se distinguem por diversos atributos, tais como:

- tipo de blockchain utilizado;
- formas de autenticação/mineração e custos envolvidos;
- restrições de emissão;
- utilidade econômica.

¹⁰ BLANDIN, A. et al. *Global Cryptoasset Regulatory Landscape Study*. University of Cambridge, Centre for Alternative Finance, 2019. Tradução livre dos autores.

Para estabelecer um arcabouço regulatório, organizações internacionais (como a OCDE) e centros de estudos (como o CCAF¹¹) classificam *tokens* em categorias amplas, de acordo com sua utilidade econômica, dentre as quais pode-se citar:

- Meio de pagamento (*Payment/Exchange Tokens*);
- Securitização (*Security/Equity Tokens*);
- Atribuição de posse (*Non-fungible Tokens*);
- Atribuição de direitos (*Utility Tokens*).

A classificação por utilidade econômica, em desenvolvimento, possui ainda grandes desafios. Essa segmentação não abrange todos os ativos: exclui-se dela, por exemplo, documentos, arquivos de mídia e nomes de domínio criptografados. Muitos dos *tokens* podem se inserir em mais de uma dessas categorias, sendo considerados *tokens* híbridos; e mesmo *tokens* classificados dentro das categorias mencionadas podem ter funções diversas e possuírem funções diferentes dos originalmente designados ao decorrer do tempo.

Apesar dessas dificuldades, utiliza-se neste trabalho a divisão por utilidade econômica como ferramenta para descrever alguns dos principais criptoativos e seu tratamento regulatório e tributário recebidos.

O referido tratamento tributário é em grande parte afetado pelo elevado grau de complexidade. As diversas classificações desses ativos – além da ausência de um consenso – e de suas formas de transação dificultam o desenvolvimento de um arcabouço comum. Essa ausência de diretrizes é também afetada pela natureza dinâmica dos ativos em questão, sujeitos a um elevado número de inovações tecnológicas e econômicas¹².

Nas seções a seguir, serão apresentados os principais tipos de criptoativos, bem como um tipo de agente que merece atenção nesse mercado¹³: as *exchanges*. O

¹¹ Cambridge Center for Alternative Finance (CCAF), é um grupo de estudos da Cambridge Judge Business School para finanças alternativas. Utiliza-se como uma das fontes desta subseção o relatório *Global Cryptoasset Regulatory Landscape Study*, disponível em <https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/cryptoasset-regulation/#.YxeTN3bMLIU>. Acesso em 06/09/2022.

¹² Fonte: OCDE. *Taxing Virtual Currencies: An Overview of Tax Treatments and Emerging Tax Policy Issues*. Disponível em: <https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.htm>. Acesso em 16/09/2022.

¹³ Com o crescimento da criptoeconomia diversos desses agentes econômicos se tornaram empresas de grande porte com efeitos significativos na economia geral, por seus efeitos sobre emprego, renda, perfil de investimentos e arrecadação tributária.

delineamento desse processo de diversificação do setor será complementado com uma apresentação de sua expansão nos anos recentes, de modo a apontar, em um plano geral, a complexidade inerente a questões regulatórias e tributárias.

2.1.1 Payment Tokens (ou tokens de pagamento)

De forma ampla, os *payment tokens* são definidos como meios de troca que podem ser utilizados como meios de pagamento. Dentro dessa definição e para os propósitos deste trabalho há dois tipos de *tokens* de pagamento que podem ser destacados.

O primeiro elemento dessa tipologia são as criptomoedas não lastreadas. Estas podem ser definidas como ativos sem contraparte devedora, emissor e promessa de retorno¹⁴. Quando utilizados como ativos de investimento, podem ser classificados como ativos híbridos, como é o caso do Bitcoin e do Ether.

O segundo elemento da tipologia são as criptomoedas lastreadas, cujo valor é determinado a partir de uma relação de paridade com algum ativo real ou uma relação de garantia, concedida pela instituição responsável por sua emissão. As criptomoedas lastreadas abrangem, fundamentalmente, dois tipos de ativos:

- As *stablecoins*, que são ativos cujo preço é pareado com moedas fiduciárias, são assim denominadas por não apresentarem a volatilidade de valor das criptomoedas não lastreadas¹⁵.
- Os CBDCs (*Central Bank Digital Currency*), que são instrumentos de pagamento digitais, criados em blockchains privados por bancos centrais. Tais ativos são denominados na unidade nacional de conta, que constitui um passivo do Banco Central.

O advento das CBDCs apresenta um conjunto de novas funcionalidades ao mercado de criptoativos, além de possibilitar transações em moeda análoga à fiduciária sem

¹⁴ Segundo classificação do FMI esses ativos também podem ser denominados “*Bitcoin Like Cryptoassets*” (BLCA) e são definidos por terem sido projetados para servir como meio de troca em pagamentos entre pessoas, além de não possuírem emissor ou contraparte devedora (Tradução livre de: “*are designed to serve as a general-purpose medium of exchange for peer-to-peer payments, with no issuer and no counterpart liability*”).

¹⁵ As *stablecoins* também podem ser divididas em categorias. Fundamentalmente, pode-se separá-las em dois grupos: lastreadas (com variação pareada a algum ativo específico, como moedas fiduciárias, outros criptoativos e commodities) e algorítmicas (que têm sua estabilidade alcançada a partir do uso de algoritmos e contratos inteligentes).

intermediários financeiros. Dentre as novas funcionalidades¹⁶ mencionadas, cabe destacar:

- Maior eficiência de pagamentos: potencial de se oferecer meios de pagamentos com baixo custo como um bem público.
- Novas funções de pagamento e liquidação de dívidas, oferecidas a uma gama muito mais ampla de intermediários do que apenas os bancos comerciais domésticos.
- Maior acessibilidade à entrada de agentes (famílias e empresas) nesse mercado, ao nível de varejo.
- Desbloqueio a inovações no setor privado, através de um amplo conjunto de serviços.

Todas as inovações mencionadas permitem um estímulo à competição entre agentes e a uma diversificação ainda maior de ativos e funcionalidades. Isso se dá, fundamentalmente, pelo fato de que possibilitam a realização de transferências sem intermediários. Esse processo é intensificado pela existência das CBDCs, uma vez que ampliam ainda mais o escopo de agentes e instituições envolvidos no processo de digitalização dos ativos.

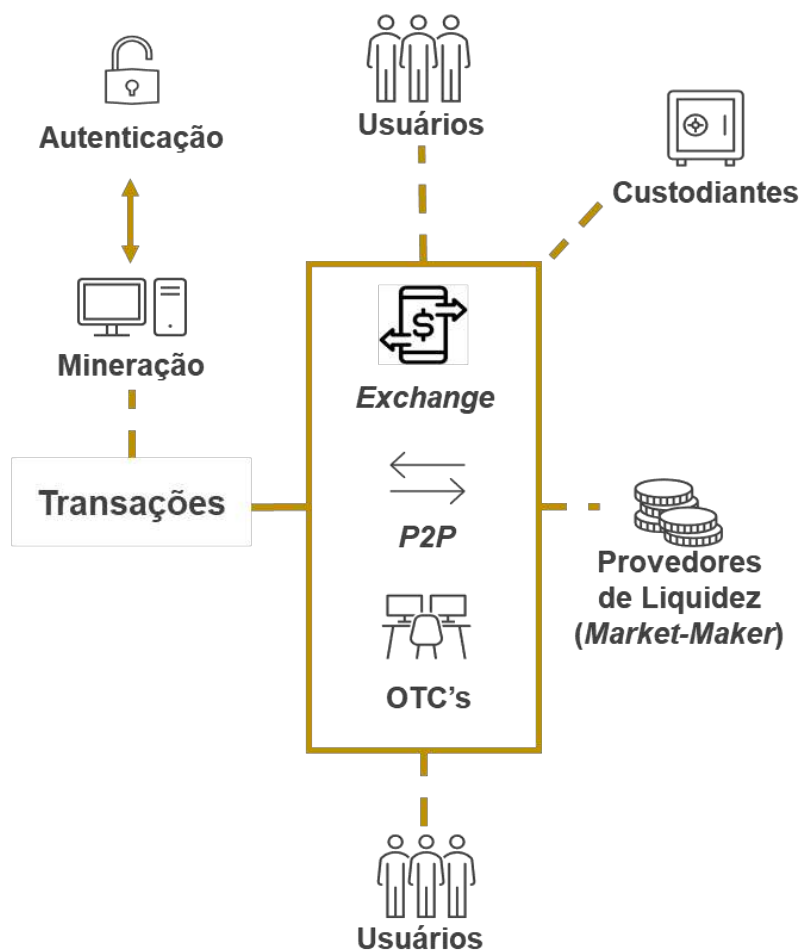
Na Figura 1 é apresentado um diagrama que descreve operações com *tokens* de pagamento, destacando seus principais agentes e os formatos de transações, dos quais, para os propósitos deste trabalho, destaca-se:

- Transações P2P são o formato original de troca de criptoativos, via blockchain sem a presença de intermediários;
- Transações *Over the Counter* (OTC) são as compras e vendas por meio de acordos bilaterais, não públicos, para blocos maiores de operações;
- Custodiantes operadores que mantem a custódia dos ativos;
- *Market-makers* são os operadores que provém liquidez ao mercado comprando e vendendo grandes volumes de ativos aos *players* que demandarem¹⁷.

¹⁶ Fonte: *BIS: The Future of The Monetary System*. Relatório do BIS acerca das novas tendências inerentes ao sistema monetário internacional, dentre as quais destaca-se a digitalização de ativos, com grande ênfase às CBDCs. Disponível em: <https://www.bis.org/publ/arpdf/ar2022e3.pdf>. Acesso em: 15/09/2022.

¹⁷ Os serviços de custódia e *market-making* também são costumeiramente prestados por *exchanges*, de forma que, muitas vezes, tais empresas se tornam centrais nas atividades ligadas a criptoeconomia. A atividade dos mineradores foi apresentada no Box 1 deste estudo.

Figura 1: Diagrama representativo de operações envolvendo *tokens* de pagamento



Elaboração: LCA Consultores.

2.1.2 Outros Tokens

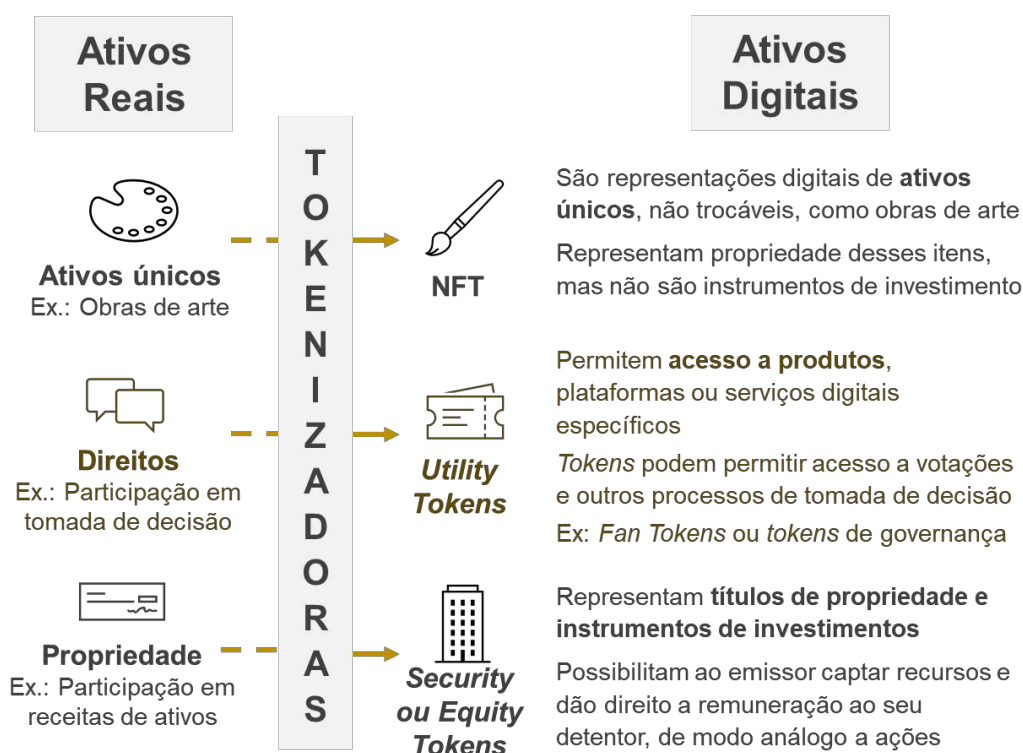
Para além dos *tokens* de pagamento, há outras categorias de *tokens*, que são classificadas de acordo com a função específica que desempenham, diversificando-se em relação ao uso exclusivo como meio de pagamento ou reserva de valor. Nesta seção, esses outros *tokens* serão apresentados de forma mais detalhada.

De acordo com a Anbima (Associação Nacional das Entidades dos Mercados Financeiro e de Capitais), a transformação de ativos “físicos” ou “reais” em ativos digitais é

chamada de tokenização¹⁸. Esse processo é realizado pelas empresas tokenizadoras, que funcionam como agentes “estruturadores” do mercado de criptoativos¹⁹.

A dinâmica de tokenização permite a venda de direitos e recebíveis que de outro modo seriam ilíquidos, diversificando ainda mais o mercado de criptoativos. A Figura 2 apresenta alguns exemplos de tipos dos ativos *tokenizados* (NFTs, *Utility Tokens* e *Security* ou *Equity Tokens*).

Figura 2: Esquemática de tokenização de ativos únicos, direitos e propriedade



Elaboração: LCA Consultores.

¹⁸ Anbima (2022) *Tokenização de Ativos: Conceitos iniciais e experimentos em curso*. Disponível em <https://www.anbima.com.br/data/files/02/30/82/CB/68001810C27A8F08882BA2A8/Tokenizacao%20de%20ativos.pdf>. Acesso em 08/09/2022.

¹⁹ De acordo com a Anbima (2022) o processo de estruturação do mercado de criptoativos se dá a partir de um conjunto de atividades, como: escrituração, oferta, intermediação, distribuição, custódia e liquidação de produtos tokenizados.

Box 2: Outras aplicações para a tecnologia blockchain

Devido à característica incipiente da maior parte das tecnologias, os desdobramentos da criptoeconomia para os demais setores da economia ainda são incertos em escopo e magnitude. Vislumbra-se, porém, diversas aplicações potenciais da tecnologia blockchain e do processo de tokenização através de setores distintos, além de aplicações já em desenvolvimento nos setores público e privado. Apresenta-se neste Box dois dos ramos de aplicação.

Cadeia de suprimentos

A tecnologia de blockchain pode ser utilizada para conferir rastreabilidade à cadeia de alimentos, por exemplo, promovendo informações como: local de produção, percurso dos alimentos, agrotóxicos, remuneração dos empregados, dentre outras.

- JBS: Uso de plataforma pecuária transparente para monitoramento de desmatamento e uso de mão de obra nos locais de produção²⁰.
- IBM Food Trust: Rastreamento de produtos e lotes, sobretudo em parceria com a rede Walmart, atualmente nas cadeias do café, de pesca, dentre outras²¹.
- FedEx: integrou o blockchain à sua cadeia de custódia, com o intuito de melhorar a rastreabilidade e gerar registros mais confiáveis, o que auxilia em disputas judiciais frente a consumidores²².
- Bumble Bee Seafood Co.: utilização de plataforma na blockchain para rastrear o trajeto de peixes, desde o momento da pesca até chegar ao consumidor final²³.

Digitalização Segura

Redes em blockchain também podem ser utilizadas por governos e empresas visando modernização do processo de registros, como por exemplo:

- Receita Federal do Brasil – Rede em blockchain em fase de testes facilita compartilhamento e autenticidade de dados do CPF e CNPJ²⁴.

²⁰ Fonte: <https://jbs.com.br/saiba-mais/blockchain/>. Acesso em 12/09/2022.

²¹ Fontes: <https://www.hyperledger.org/learn/publications/walmart-case-study> e <https://www.ibm.com/br-pt/blockchain/solutions/food-trust>. Acesso em 12/09/2022.

²² Fonte: <https://www.forbes.com/sites/forbestechcouncil/2021/11/08/blockchain-in-supply-chain/?sh=307c83f74e1a>. Acesso em: 28/09/2022.

²³ Fonte: <https://thebumblebeecompany.com/bumble-bee-foods-and-sap-create-blockchain-to-track-fresh-fish-from-ocean-to-table/>. Acesso em: 28/09/2022.

²⁴ Fonte: <https://exame.com/future-of-money/blockchain-e-dlts/receita-federal-adota-rede-blockchain-do-mercosul-para-o-comercio-exterior/>. Acesso em 16/09/2022.

- Governo do Ceará – Tecnologia blockchain em desenvolvimento para registro e monitoramento de transações em obras públicas²⁵.
- Governo da Estônia: Governo estima economizar cerca de 2% do PIB por ano com assinaturas digitais em blockchain, através da redução de custos cartoriais. Governo estoniano também se posiciona como referência em identificação digital e armazenamento de informações relativas à saúde²⁶.

2.2 Evolução do mercado mundial de criptoativos

O período pós-2018 é marcado por intensa valorização de mercado dos criptoativos de maior proeminência, como o Bitcoin (variação de 179% de março 2018 a setembro de 2022) e o Ethereum (232%), bem como pelo surgimento de centenas de novos criptoativos. Esse processo de expansão se intensifica principalmente entre os anos de 2020 e 2021, com uma inflexão vertiginosa no valor de mercado de criptoativos no mundo. O desenvolvimento de novos tipos de criptomoedas, bem como suas novas aplicações e a maior demanda por ativos de risco estão entre os fatores explicativos do expressivo crescimento observado no Gráfico 2.

²⁵ Fonte: <https://cointelegraph.com.br/news/government-of-ceara-develops-blockchain-platform-to-prevent-fraud-in-public-works>. Acesso em 16/09/2022.

²⁶ Fonte: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/08/como-estonia-construiu-uma-sociedade-digital.html>. Acesso em 12/09/2022.

Gráfico 2: Valor de capitalização de mercado dos criptoativos no mundo (em US\$ bilhões), de março de 2018 a setembro de 2022



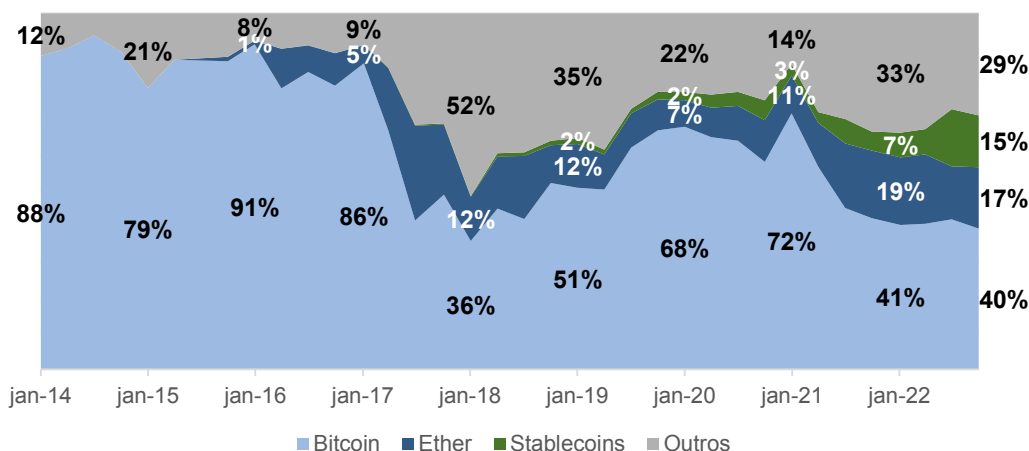
*Nota: O valor de capitalização de mercado é uma métrica que calcula o valor de mercado de um ativo, multiplicando o seu preço pelo seu volume disponível (exemplo: número de bitcoins*preço do bitcoin). O dado apresentado considera todos os criptoativos, incluindo stablecoins e tokens. É, portanto, distinto e superior ao valor correspondente ao volume negociado em 24 horas. Fonte: CoinMarketCap. Elaboração: LCA Consultores.*

Como observado no Gráfico 3, o Bitcoin ainda é o criptoativo predominante, mas observa-se crescente diversificação dentre os ativos. Ressalta-se, a partir de 2016, o surgimento da rede Ethereum, direcionada para contratos inteligentes e aplicações descentralizadas, e a consequente proeminência do Ether como segundo criptoativo em valor de mercado²⁷.

Outro movimento visível no gráfico é a criação e desenvolvimento das *stablecoins*, que tiveram ganho de valor relativo significativo no período. É possível apontar alguns possíveis determinantes desse processo, a começar pelo fato de que as *stablecoins* são instrumentos que têm aplicabilidade no lado real da economia, e se distinguem de outros criptoativos pelo maior grau de segurança garantida aos agentes. Tais ativos podem ser considerados, portanto, um bom substituto para ativos tradicionais, além de representarem uma forma bastante útil de aplicação da tecnologia aqui discutida, fatores que, conjuntamente, impulsionam o uso dessa classe de ativos.

²⁷ Devido a volatilidade dos ativos há uma variação diária significativa no valor de capitalização de cada um dos destes, não captada pelo gráfico.

Gráfico 3: Participação no valor de capitalização de mercado, por criptoativo (janeiro de 2014 a outubro de 2022)²⁸



Nota: As stablecoins consideradas foram as de maior capitalização em jan/22: Tether, USD Coin e Binance USD. Fonte: CoinMarketCap. Elaboração: LCA Consultores.

Em síntese, é possível observar por ambos os gráficos, dois movimentos simultâneos: a expansão das transações e do uso de criptoativos; e a diversificação dos tipos de criptoativos existentes, bem como de suas respectivas funções.

Parte desse processo é reflexo da complexificação derivada da tokenização de ativos, destacando sobretudo o desenvolvimento de *stablecoins* como uma das forças relevantes no movimento de diversificações de ativos, conforme descrito anteriormente. Enfatiza-se também o surgimento de uma série de novas funcionalidades inerentes à utilização dos *tokens*, os quais ganham aplicabilidade em vários segmentos da economia²⁹, como por exemplo o sistema de finanças descentralizadas (DeFi)³⁰.

²⁸ Informações relativas ao primeiro dado disponível de cada mês.

²⁹ Fonte: BIS: The Future of The Monetary System. Disponível em: <https://www.bis.org/publ/arpdf/ar2022e3.pdf>. Acesso em: 15/09/2022.

³⁰ Dentre essas funcionalidades, destaca-se o sistema de finanças descentralizadas (DeFi), no qual contratos inteligentes possibilitam contrair empréstimos e seguros sem nenhuma intermediação centralizada. O sistema DeFi é uma ferramenta do universo cripto que permite a geração de uma oferta de serviços e produtos financeiros com potencial de desenvolver o sistema financeiro ao retirar intermediários e, com isso, custos de transação. A diversificação de ativos é fundamental para consolidar o sistema DeFi, uma vez que permite incentivos à inovação e à eficiência. Esse processo ocorre com algumas garantias de estabilidade, que se dá pela existência de ativos como as *stablecoins*, as quais vêm atraindo parte cada vez mais significativa da demanda por criptoativos.

2.3 Exchanges de criptoativos

As *exchanges*, como já mencionado acima, podem ser definidas como plataformas que atuam como intermediárias em transações de criptoativos, se apresentando como alternativas às negociações P2P. Tais instituições realizam transações públicas e transparentes, em um livro de ordens análogo a um mercado tradicional. Dentre as vantagens oferecidas pelas *exchanges* quando comparadas às transações P2P ou em OTCs, destacam-se:

- Capacidade de redução dos custos de transação, principalmente no tocante à oferta e demanda por criptoativos, dado que a existência de uma plataforma permite a conexão de compradores e vendedores de forma mais eficiente.
- Redução de assimetria de informação, que se dá pela garantia às partes envolvidas de que as operações serão liquidadas.

As *exchanges* são o foco principal da análise tributária e regulatória deste estudo. Dessa forma, a investigação se concentra apenas em transações públicas (intermediação e saque) feitas por plataformas de intermediação, sem abarcar transações do tipo P2P, em OTCs, DEX e serviços de tokenização. A restrição da análise decorre da dificuldade de identificação dos agentes que realizam operações com criptoativos fora do escopo de atuação das *exchanges*, dada a escassez de dados públicos sobre tais atividades.

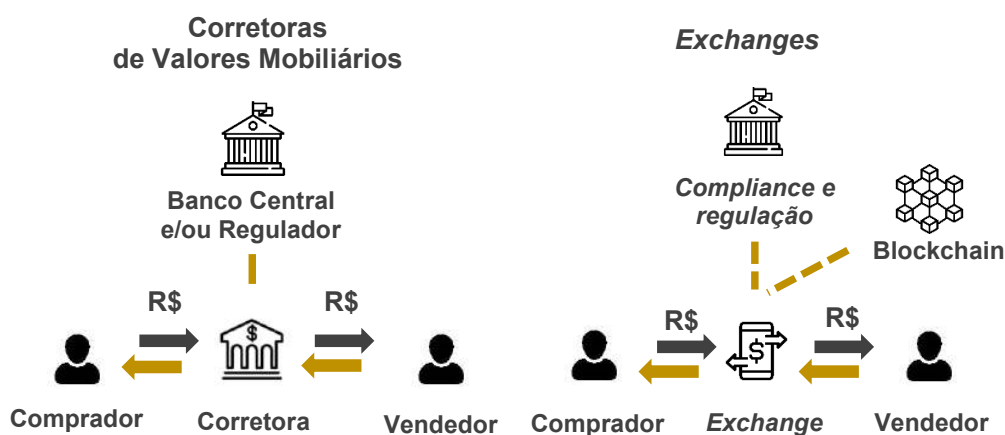
As *exchanges* de criptoativos realizam serviços diversos, dentre os quais cabe destacar:

- Venda direta de criptoativos. É organizada através da compra ou venda de criptoativos de *market-makers*³¹ e outros agentes, ligando-os aos clientes.
- Intermediação de transações de criptoativos. Conecta dois clientes, ofertando o serviço de *matching* entre comprador e vendedor. Parte das receitas das *exchanges* advém de taxas cobradas sobre essas transações, chamadas de taxas de ordem.
- Armazenamento: é uma função realizada por custodiantes e *exchanges*, permitindo compra e venda de criptoativos utilizando carteiras próprias.

³¹ Como explicado acima, *market-makers* são os agentes responsáveis por garantir liquidez e profundidade ao mercado de determinado ativo. Tais agentes atuam transacionando esse ativo, e têm seus lucros derivados do *spread* produzido pela diferença entre ofertantes e demandantes no mercado. As *exchanges* de criptoativos podem atuar também como *market-makers*.

A maior parte das *exchanges* de criptoativos adota um modelo de negócios centralizado, atuando, como já dito, como uma plataforma intermediária entre agentes no mercado de criptoativos. Como se pode ver na Figura 3 esse tipo de modelo de negócio se assemelha muito ao das corretoras de valores mobiliários. Além das *exchanges* centralizadas, contudo, há também as plataformas descentralizadas (DEX), que operam através de um protocolo de *smart contracts* na blockchain

Figura 3: Dinâmicas de funcionamento de *exchanges* de criptoativos e corretoras de valores mobiliários



Elaboração: LCA Consultores.

Dentre as *exchanges* com maior *share* mundial (em valor transacionado), grande parte tem sede em paraísos fiscais ou países com regime fiscal privilegiado³², como a Binance, sediada nas Ilhas Cayman, ou a FTX, sediada nas Bahamas. Na seção 4 a problemática regulatória que envolve esse tema é aprofundada.

Destaca-se, no entanto, uma incipiente reversão nos anos recentes, em decorrência de pressões regulatórias de alguns países. O caso mais notável é dos Estados Unidos, que passaram a condicionar as operações de grandes *exchanges* à existência de sedes locais que se comportem de acordo com as normas regulatórias do país. Isso pode ser visto na Tabela 1, na qual constam a Binance e a Binance US, *exchange* vinculada à Binance, mas com operação exclusiva nos EUA. Vale destacar que o mercado de

³² Segundo definição da Instrução Normativa N° 1037, de 04 de junho de 2010 Ilhas Cayman, Bahamas, Hong Kong e Seychelles são paraísos fiscais, enquanto Malta é um regime fiscal privilegiado para: *International Trading Company* (ITC) e de *International Holding Company* (IHC).

criptoativos possui elevada volatilidade, de modo que o volume transacionado por *exchange* pode apresentar flutuações diárias muito elevadas.

Tabela 1: Sedes das 10 maiores *exchanges* do mundo, por *exchange score*

Exchange	Sede
Binance	Ilhas Cayman ¹
FTX	Bahamas
Coinbase	Estados Unidos
Kraken	Estados Unidos
Gate.io	Estados Unidos
KuCoin	Seychelles
Binance.US	Estados Unidos
Huobi	Seychelles
Bitfinex	Ilhas Virgens
bitFlyer	Japão

Nota: 1. Não há clareza quanto a sede fiscal da Binance. 2. A tabela em questão apresenta as maiores exchanges do mundo por exchange score, em 25/07/2022. Fonte: CoinMarketCap. Elaboração: LCA Consultores.

De todo o exposto nesta seção, vale destacar:

- Mercados da criptoeconomia estão em pleno desenvolvimento e apresentam características disruptivas que trazem novidades e incertezas;
- Esse cenário apresenta significativas implicações regulatórias e tributárias, dificultando a construção de diretrizes amplas e sistemáticas para o setor;
- O mercado de criptoativos tem apresentado duas tendências recentes: o aumento do valor dos ativos; e de diversificação dos tipos de ativos existentes, bem como suas respectivas funções;
- *Exchanges* situadas em paraísos fiscais são comuns no mercado de criptoativos.

3. Criptoeconomia e *exchanges* no Brasil

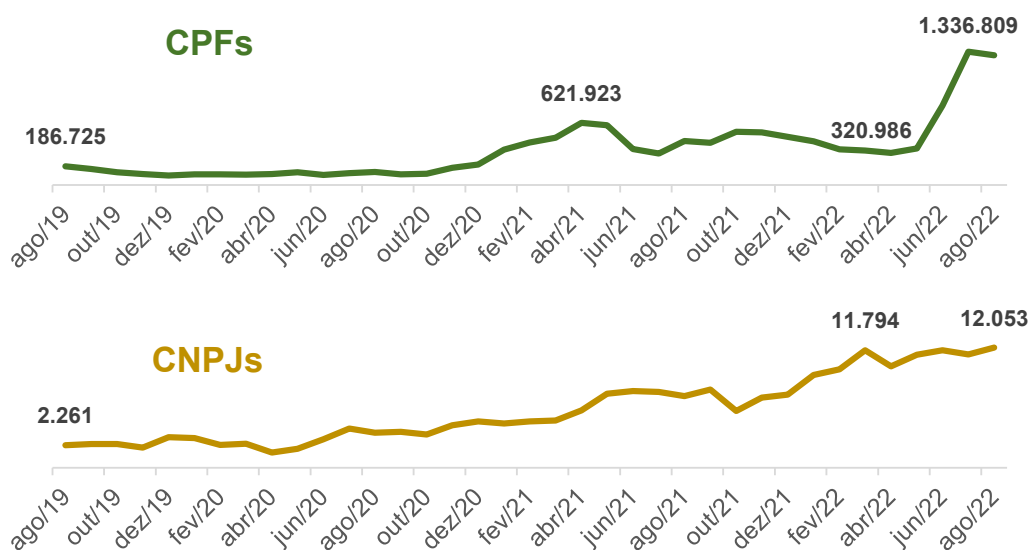
A presente seção visa apresentar dados gerais da criptoeconomia e da operação de *exchanges* no Brasil. Para tal ela se divide em três partes: a primeira objetiva apresentar dados gerais relativos ao mercado de criptoativos no Brasil, a segunda estuda o fluxo internacional desses ativos e a terceira visa dimensionar o mercado nacional de transações e saques de criptoativos. Dentro desta última é relevante segmentar os agentes, para tal será apresentada a metodologia utilizada bem como a razoabilidade da diferenciação. Parte dos resultados aqui apresentados servirão de base para os cálculos relativos à estimativa tributária, expostos na Seção 5.

3.1 Indicadores de evolução do mercado e participação por criptoativos

Segundo informações declaradas à Receita Federal do Brasil³³, o mercado de criptoativos cresceu de modo expressivo nos últimos anos, incluindo cada vez mais pessoas e empresas. Conforme apresentado no Gráfico 4, o número de CPFs declarantes de transações com tais ativos atingiu valor recorde, de 1.336.809 pessoas físicas, em julho de 2022. O número de CNPJs, por sua vez, mostrou uma tendência de crescimento durante todo o período, atingindo o valor máximo de 12.053 pessoas jurídicas declarantes em agosto de 2022, a última observação da série.

³³ O órgão congrega informações declaradas por pessoas físicas e jurídicas, em conformidade com a IN 1.888/2019, mesmo quando as operações são feitas fora do livro aberto (realizadas em OTCs e parte das operações P2P, que representam aproximadamente 16% do total declarado). Parte dos operadores no Brasil não possuem domicílio fiscal no país, sendo incerta sua conformação à IN, de modo que esses dados retratam apenas uma parte do mercado nacional. Essa discussão será aprofundada no decorrer desta seção e no Anexo 4, que explica em maior detalhe os possíveis vieses da base de dados da Receita Federal, comparando-a com fontes alternativas, os sites agregadores de transações de criptoativos em *exchanges*.

Gráfico 4: Número de CPFs e CNPJs únicos declarantes de negociações com criptoativos (em milhares), de agosto de 2019 a agosto de 2022



Fonte: Receita Federal do Brasil. Elaboração: LCA Consultores.

Quanto ao perfil dos detentores de criptoativos, estudo da TripleA (2021) estima que 5% da população nacional possua criptoativos, possibilitando um contingente de 10,4 milhões de proprietários³⁴. Segundo os dados declarados à RFB, cerca de 87% das operações com criptoativos no Brasil em 2021 foram feitas por pessoas do sexo masculino³⁵.

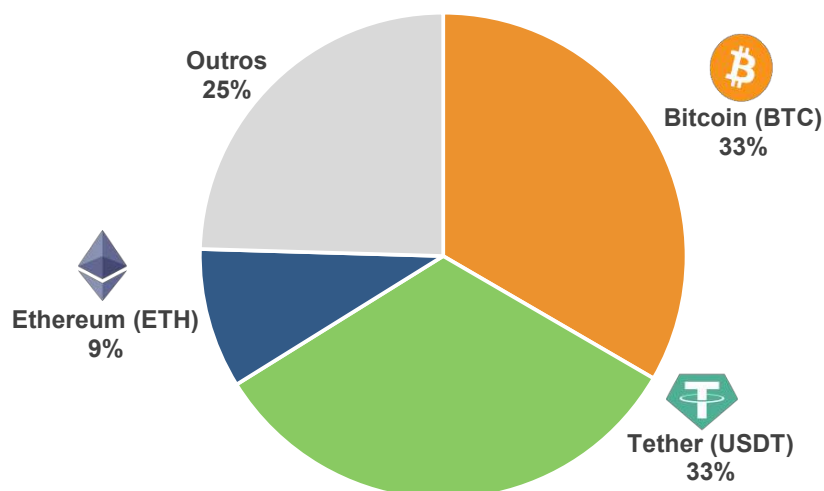
Ainda nesse período, o Bitcoin e o Tether foram proporcionalmente os criptoativos mais transacionados no país, dentre os tipos negociados nas transações declaradas à RFB. Como mostra o Gráfico 5, cada um dos ativos correspondeu a cerca de um terço do valor de criptoativos transacionados declarados no período. Nota-se que nos valores declarados à RFB existe uma participação maior de *stablecoins* do que na capitalização de mercado mundial apresentada na Seção 2³⁶.

³⁴ TripleA (2021) *Cryptocurrency across the world*. Disponível em: <https://triple-a.io/crypto-ownership-brazil/>. Acesso em: 28/09/2022.

³⁵ O valor médio calculado das operações foi de R\$ 68,77 para o sexo masculino e de R\$ 68,41 para o feminino.

³⁶ A tendência das transações apresentadas nos agregadores, sites que agregam dados do mercado, é de menor participação de *stablecoins*, como o Tether (o Anexo 4 explica detalhadamente o que são agregadores e suas diferenças para dados da RFB). Como mostrado pelo gráfico, nos dados declarados à RFB a proporção de Bitcoin e Tether é de 33% para ambos, já no *Livecoins*, agregador utilizado na metodologia de dimensionamento de mercado (apresentada abaixo), as participações são respectivamente de 32,6% e de apenas 3,5%. Tal comparação mostra que existe uma tendência maior de declaração de *stablecoins*, tais como o Tether. A proporção de Bitcoins nas transações de ambas as fontes é semelhante, indicando não existir viés na escolha das *exchanges* para transações desses ativos, premissa importante para

Gráfico 5: Proporção, por criptoativo utilizado, do valor transacionado declarado (2021)



*Nota: "Outros" inclui demais criptoativos declarados para a RFB (como USDC, CHZ, dentre 60 outros).
Fonte: Receita Federal do Brasil. Elaboração: LCA Consultores.*

Box 3: Índícios de geração significativa de empregos em empresas nacionais ligadas a criptoeconomia

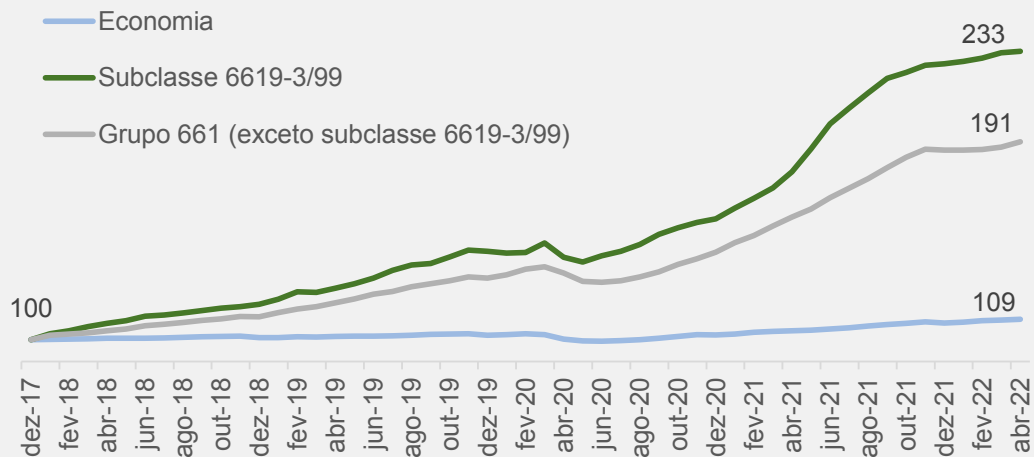
A partir de dados públicos, conforme apresentado no Gráfico 6, pode-se notar que a CNAE subclasse 6619-3/99³⁷, que engloba o setor de transação de criptoativos, teve desempenho bastante superior à economia e às outras subclasses pertencentes ao mesmo grupo (661), para o período analisado³⁸.

o dimensionamento de mercado apresentado a seguir (a segmentação entre *exchanges* é mais bem explicada e justificada na seção 3.1.1 deste estudo). Por fim cabe notar que o período de coleta dos dados apresentados é ligeiramente diferente, sendo os dados da RFB referentes ao ano completo de 2021 e os oriundos do *Livecoins* restritos ao segundo semestre do mesmo ano, devido à restrição de acesso a outras informações.

³⁷ A CNAE 6619-3/99, "Outras atividades auxiliares dos serviços financeiros não especificadas anteriormente", engloba, entre outras atividades, custódia e cessão temporária (locação) de criptoativos. Dentre tais outras atividades podem-se citar: casas de câmbio, plataformas de pagamento online, corretagem de consórcios, corretor hipotecário.

³⁸ O Grupo 661 "Atividades auxiliares dos serviços financeiros" é o que engloba a subclasse em questão, por isso a comparação com ele pode mostrar de que forma o mercado cripto se destacou de atividades comparáveis.

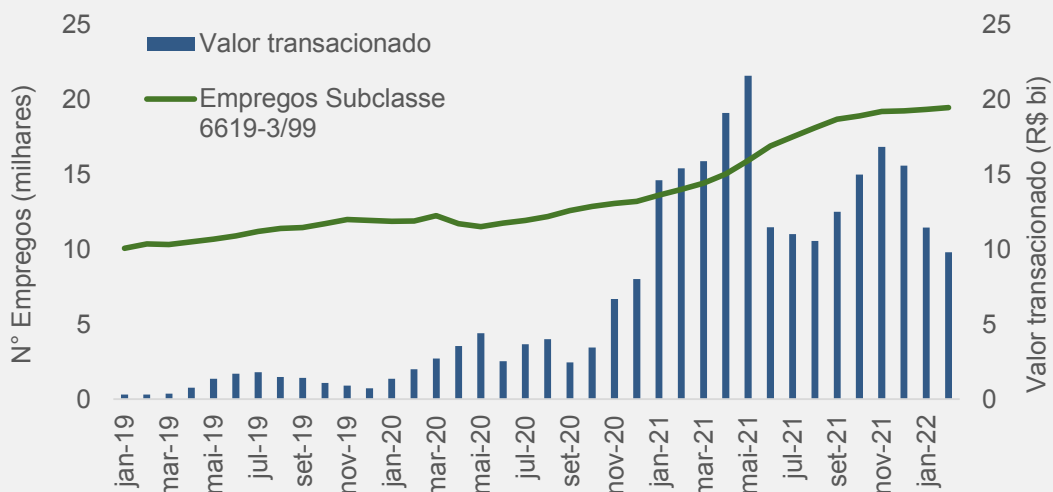
Gráfico 6: Evolução comparada do número de vínculos empregatícios (dez/2017 = 100) de dezembro de 2017 a abril de 2022



Nota: Os dados da CNAE grupo 661 excluem a subclasse 6619-3/99 para esclarecer a comparação entre as atividades. Fontes: CAGED e RAIS. Elaboração: LCA Consultores.

Conforme exposto no Gráfico 7, entre janeiro de 2019 e fevereiro de 2022 o número de empregos da CNAE 6619-3/99 dobrou em magnitude, com geração de cerca de 10 mil vagas. Tal cenário coincide com o período de maior crescimento das transações com criptoativos por brasileiros, fator que pode apontar contribuição da criptoeconomia para o crescimento do número de vagas formais na CNAE em questão.

Gráfico 7: Comparação da evolução de vínculos da CNAE 6619-3/99 com o valor de criptoativos transacionados por exchanges no Brasil de janeiro de 2019 a abril de 2022



Fontes: CAGED, RAIS, CoinTradeMonitor e RFB. Elaboração: LCA Consultores.

Ainda que não se possa creditar a totalidade desses empregos gerados à criptoeconomia, pode-se dizer que há indícios de geração significativa de empregos em empresas ligadas a ela.

Existem ainda alguns vínculos formais no setor que não são identificados pela análise apresentada acima, como por exemplo em *exchanges* que não estão registradas na CNAE subclasse analisada³⁹. Por fim, é esperado que um setor que movimenta cifras da ordem de bilhões de reais (como será apresentado ainda nesta seção) gere empregos de maneira indireta, como através do desenvolvimento de tecnologias de suporte e outras atividades auxiliares.

3.2 Importações

Os dados relativos ao comércio exterior de criptoativos são computados pelo Banco Central do Brasil (BCB), autarquia federal que controla, entre outros, o mercado cambial. O órgão estima a importação e exportação de criptoativos através dos contratos de câmbio em moeda fiduciária entre as partes⁴⁰, de tal maneira que as estimativas do BCB não captam transações entre criptoativos, observando apenas ações de *market-makers* domiciliadas no Brasil⁴¹.

A série histórica é divulgada pela autoridade monetária brasileira no balanço de pagamentos, seguindo recomendação do FMI⁴². Mais especificamente o órgão internacional recomenda incluir transferência de propriedade de criptoativos entre residentes e não residentes na conta de bens do balanço.

Através do Gráfico 8 fica visível o crescimento das importações, principalmente a partir de 2018. Tal valor será útil também na Seção 5, na qual serão apresentadas as estimativas de arrecadação de tributos. Enquanto isso, não existem exportações de ordem de grandeza próxima devido à baixa rentabilidade da atividade de mineração em solo brasileiro, causada pelo elevado custo energético nacional. O valor total importado em 2021 é de 6 bilhões de dólares, equivalente a 32,2 bilhões de reais⁴³.

³⁹ O Anexo 1 apresenta a relação de empresas registradas na subclasse 6619-3/99, segmentando-as entre: não registradas, registradas como atividade primária e registradas como atividade secundária.

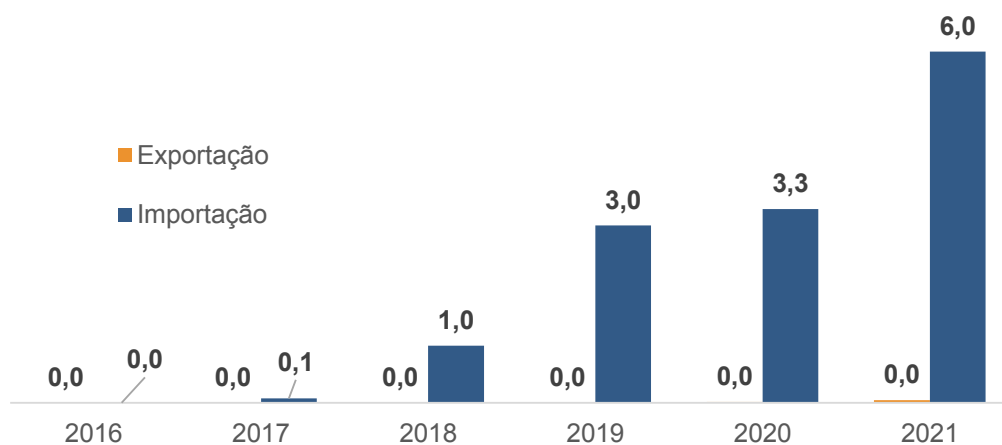
⁴⁰ Vale destacar que, como essa é a metodologia empregada pelo BCB, implica-se que há pagamento de IOF câmbio por parte das negociantes. Essa premissa será melhor apresentada e discutida na seção 5 deste estudo.

⁴¹ Supõe-se que agentes internacionais realizam operações utilizando apenas criptoativos, de forma que o número total de importações deve ser superior ao estimado pelo BCB.

⁴² Em concordância com as diretrizes do FMI, o BCB classifica criptoativos como ativos não financeiros, uma vez que eles não possuem contraparte devedora

⁴³ Conversão feita através da taxa de câmbio comercial média mensal (Banco Central do Brasil).

Gráfico 8: Estimativa do BCB de exportação e importação de criptoativos (em US\$ bilhões) de 2016 a 2021



Fonte: Banco Central do Brasil. Elaboração: LCA Consultores.

3.3 Dimensionamento de mercado

Através de dados públicos é possível dimensionar o mercado de transações realizadas por *exchanges* no Brasil, objetivo deste estudo, conforme apresentado na seção 2. O objetivo dessa subseção é apresentar tais resultados e as metodologias que levaram aos mesmos. É apresentada ainda uma importante distinção realizada entre as *exchanges* que atuam no Brasil, segmentando-as entre quatro modelos de negócios.

3.3.1 Classificação das *exchanges* no Brasil

Para os propósitos deste trabalho, se faz relevante a segmentação das *exchanges* que atuam no mercado brasileiro entre alguns modelos de negócios. Esse tratamento é necessário devido a eventuais diferenças na capacidade de órgãos locais em aplicar normas regulatórias e tributárias para as empresas do setor. Tal desequilíbrio pode gerar distorções competitivas, dado que *exchanges* que têm a maior parte da sua operação dentro do país podem estar sujeitas a um conjunto maior de obrigações.

A divisão entre *exchanges* foi parcialmente inspirada na classificação utilizada pela Receita Federal para segmentação de seus dados abertos, na qual, segundo declarado via LAI⁴⁴, as empresas são segmentadas de acordo com domicílio fiscal.

Nesse contexto, define-se⁴⁵:

Exchanges nacionais são aquelas que possuem domicílio no Brasil, caracterizado pela presença de CNPJ e quadro societário composto por pessoas físicas e/ou jurídicas exclusivamente brasileiras. Através do uso de sites agregadores de transações⁴⁶ foram identificadas vinte e seis *exchanges* que podem ser enquadradas neste grupo em 2021.

Exchanges nacionalizadas são semelhantes às nacionais, diferenciando-se apenas por terem sido fundadas no exterior, e por terem constituído domicílio fiscal no Brasil posteriormente. Destaca-se a presença de duas *exchanges* nacionalizadas nos dados dos sites agregadores em 2021.

Exchanges parcialmente nacionalizadas são definidas como aquelas que possuem apenas empresas de intermediação financeira domiciliadas no Brasil (isso é, com CNPJ em nome próprio). Estas *exchanges* compõem o quadro societário das intermediadoras, mas por não estarem domiciliadas em território nacional entende-se que uma parte das operações é realizada no exterior. Nos dados dos sites agregadores encontram-se cinco *exchanges* sob esta classificação em 2021.

Exchanges estrangeiras não possuem operações domiciliadas no Brasil, fato observado pela ausência de CNPJ ou pela descrição da empresa como

⁴⁴ O Anexo 2 apresenta os pedidos de informação realizados via LAI, bem como as respostas dos órgãos inquiridos.

⁴⁵ A Metodologia foi construída a partir de pesquisa sobre os domicílios fiscais de cada *exchange*, considerando os locais de suas sedes, estrutura societária e se possuíam ou não CNPJ no Brasil. Definições: (i) Nacional: Fundada no Brasil; sede no Brasil; CNPJ no Brasil; quadro societário composto exclusivamente por pessoas físicas e/ou jurídicas situadas no Brasil. (ii) Nacionalizada: Fundada no exterior; sede no Brasil; CNPJ no Brasil; quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. (iii) Parcialmente nacionalizada: Fundada no exterior; sede no exterior; CNPJ no Brasil como empresa de intermediação e com quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. (iv) Estrangeira: Fundada no exterior; sede no exterior; CNPJ no Brasil como empresa domiciliada no exterior ou ausente; quadro societário composto por pelo menos uma pessoa jurídica com sede no exterior. Classificação e discussão de casos especiais no Anexo 1.

⁴⁶ O Anexo 4 apresenta informações completas sobre o que são e como funcionam os sites agregadores.

domiciliada no exterior. Tais empresas contam com a contratação de intermediadores financeiros, com os quais não possuem vínculo societário, para realizar as operações em território nacional. O grupo é composto por duas empresas em 2021.

3.3.2 Participação de mercado das *exchanges*

Para o cálculo da participação de mercado das *exchanges*, apresentado no Gráfico 9, foram utilizados dados dos agregadores, que são *sites* que computam todas as operações feitas em livro aberto, embora não observem transações realizadas por OTCs. Foram utilizados dados do *CoinTrader Monitor* e do *LiveCoins*⁴⁷, para valores transacionados em *exchanges*⁴⁸. A primeira fonte revela o valor diário de bitcoins transacionado por *exchanges*, enquanto a segunda possui uma estimativa da participação dos bitcoins no total de criptoativos transacionados nessas plataformas.

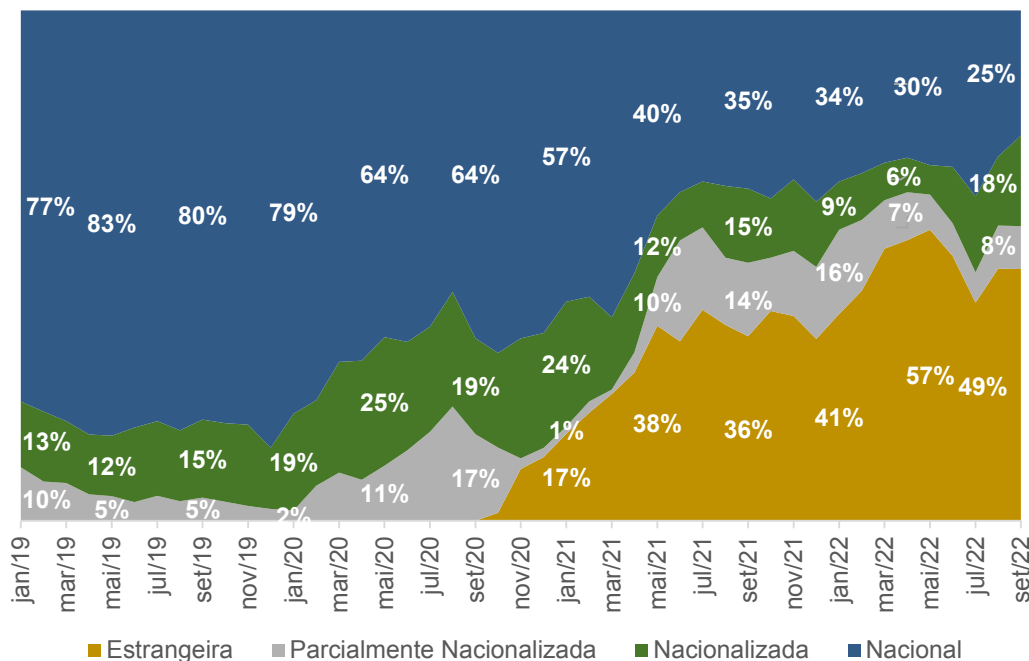
Entende-se que as transações são a melhor medida de participação de mercado, e adotou-se a premissa de que a proporção de bitcoins por total de criptoativos transacionados é igual para todas as *exchanges*⁴⁹, que modo que não há viés ao utilizar o *share* de transações de bitcoins.

⁴⁷ Para além destes utilizou-se o *Messari.io*, o *Bitcoinity* e o *Coinmetrics* em outras estimativas.

⁴⁸ Segundo a fonte: “*Esses dados são coletados diretamente das API disponibilizadas pelas próprias exchanges. Considera-se que as informações oferecidas através destes canais são DECLARAÇÕES e que não foram submetidas a auditoria externa*”.

⁴⁹ Estimada em 32,6%, média dos dados do *Livecoins* para o 2º semestre de 2021, período com informações completas de *exchanges* nacionais e internacionais.

Gráfico 9: Proporção de exchanges por classificação de janeiro de 2019 a setembro de 2022



Nota: Dados relativos a transações de Bitcoins em exchanges. Fonte: CoinTrade Monitor. Elaboração LCA Consultores.

A partir de junho de 2021, as exchanges estrangeiras passaram a constituir a maior parte do mercado brasileiro de bitcoin, sobretudo pelo impacto da entrada da Binance em outubro de 2020, ano em que as empresas estrangeiras realizaram 1,9% das transações em exchanges no Brasil. Com a participação da nova entrante, esse número saltou para 32,6% em 2021. A

Tabela 2 apresenta a participação média calculada a partir de informações do *CoinTrade Monitor* para algumas exchanges em 2021 e 2020, bem como a classificação dessas empresas. O Anexo 1 expõe de forma mais detalhada essas informações, além de apresentar o *share* das demais exchanges analisadas.

Tabela 2: Classificação e participação das 10 exchanges com maior valor transacionado em 2021

<i>Exchange</i>	<i>Classificação</i>	<i>Share 2021</i>	<i>Share 2020</i>
Binance	Estrangeira	29,8%	1,3%
BitPreço	Nacional	13,4%	12,0%
MercadoBitcoin	Nacional	13,2%	21,5%
NovaDAX	Nacionalizada	12,3%	15,1%
BitcoinToYou	Parcialmente Nacionalizada	8,7%	10,2%
Foxbit	Nacional	3,8%	5,8%
FTX	Estrangeira	2,8%	0,6%
Coinext	Nacional	2,5%	4,3%
BitcoinTrade	Nacionalizada	2,4%	6,4%
PagCripto OTC	Nacional	2,3%	0,7%

Nota: Dados relativos a transações de Bitcoins em exchanges. Fonte: CoinTrade Monitor. Elaboração LCA Consultores.

A proeminência das estrangeiras enfraquece a regulação nacional sobre as transações realizadas com criptoativos uma vez que as normas instituídas nacionalmente dificilmente se aplicam às empresas sem domicílio fiscal no Brasil. Mecanismos legais de prevenção de lavagem de dinheiro e proteção de dados, por exemplo, dificilmente são aplicados a tais *exchanges* pela ausência de jurisdição. Outro exemplo de enfraquecimento da regulação nacional se dá pela ausência de obrigatoriedade de reportar transações à RFB, sem a qual não é possível aplicar o mecanismo de prevenção de evasão fiscal conhecido como *third-party-report*⁵⁰.

⁵⁰ O mecanismo funciona através da inclusão de obrigações de conformidade de um terceiro agente, adicionalmente ao contribuinte e ao fisco. Nesse caso, o contribuinte é a pessoa física ou jurídica que executou transações com criptoativos e deve reportar seus ganhos ao fisco. O terceiro agente é a *exchange* pela qual o indivíduo realizou a transação que resultou nos ganhos. Esse mecanismo reduz os incentivos e reduz evasão fiscal, conforme apresentado no artigo *Unwilling or Unable to Cheat? Evidence From a Tax Audit Experiment in Denmark* (Kleven, Knudsen, Kreiner, Pedersen and Saez, 2011).

Esse crescimento de participação de empresas que não tem domicílio fiscal no Brasil prejudica também o potencial arrecadatório ligado a tributos sobre prestação de serviços, renda corporativa entre outros, como será mostrado na Seção 5 deste trabalho.

3.3.3 Dimensionamento das transações

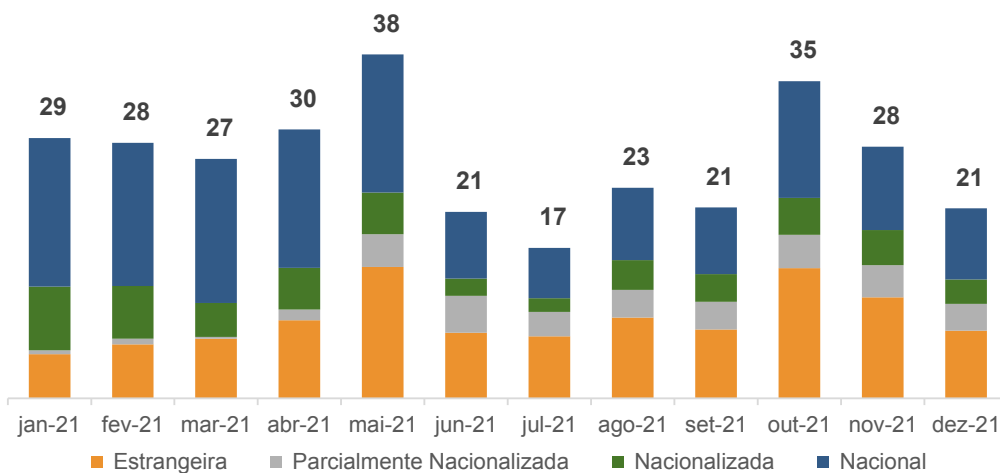
Seguindo o recorte deste estudo, apresentado na seção 2, esta subseção se propõe a dimensionar o mercado de transações em *exchanges*. Conforme dados do *Cointrade Monitor*, em 2021 foram transacionados no Brasil aproximadamente R\$ 103 bilhões em Bitcoin pelas *exchanges*⁵¹. Segundo o *Livecoins*, o Bitcoin representou 32,6% do valor total do mercado de transações de criptoativos⁵², tal percentual é também confirmado pelos dados da RFB, cuja proporção média é de 33,4% em 2021. Com essas duas informações, volume transacionado e participação de mercado do Bitcoin, é possível estimar o valor total transacionado de criptoativos, no mesmo ano: R\$ 317 bilhões, dos quais aproximadamente R\$ 137 bilhões foram transacionados em *exchanges* nacionais, R\$ 46 bi em nacionalizadas, R\$ 29 bi em parcialmente nacionalizadas e R\$ 105 bi em estrangeiras, conforme o *share* apresentado na subseção anterior. O valor total é superior a 6 vezes o estimado para 2020, de R\$ 52 bilhões.

Tais estimativas foram feitas através da participação de mercado de cada *exchange*, utilizando dados de agregadores. Os resultados dos volumes transacionados mês a mês são apresentados no Gráfico 10.

Gráfico 10: Valor total de criptoativos transacionado no Brasil, mensal em 2021, por classificação de *exchanges* (em R\$ bilhões)

⁵¹ Fonte: *CoinTrade Monitor*.

⁵² Média dos dados do *Livecoins* para o segundo semestre de 2021, período do ano com informações completas relativas as *exchanges*.



Fonte: CoinTrader Monitor e LiveCoins. Elaboração LCA Consultores.

Do panorama da criptoeconomia apresentado acima é válido destacar:

- O mercado cresceu de modo expressivo principalmente a partir de 2020, englobando cada vez mais pessoas e empresas;
- Crescimento da criptoeconomia é um dos fatores por trás da geração de cerca de 10 mil empregos na CNAE subclasse 6619-3/99 de janeiro de 2019 a fevereiro de 2022;
- Segundo o Banco Central em 2021 foram importados U\$S 6 bilhões em criptoativos;
- Houve um crescimento expressivo da participação das *exchanges* sem domicílio fiscal no Brasil (parcialmente nacionalizadas e estrangeiras) no mercado nacional em 2021. A participação de tais empresas era de 1,9% em 2020 e saltou para 32,6% em 2021;
- Estima-se que, no mesmo ano, o valor transacionado de criptoativos foi de R\$ 317 bilhões.

4. Desafios regulatórios

O surgimento de novas tecnologias impõe dificuldades para órgãos reguladores na medida que os obrigam a criar um arcabouço jurídico que possa ao mesmo tempo ser permissivo ao desenvolvimento de inovações e que proteja os consumidores. Esta seção visa apresentar parte desses desafios e introduzir discussões através da experiência internacional, na primeira subseção, e das normas vigentes e propostas ao setor no Brasil, em especial pelo PL 4.401/2021, na segunda subseção.

Para entender os possíveis benefícios da presença regulatória no setor, pode-se traçar um paralelo com os ganhos apontados na literatura especializada em uma atividade econômica comparável: os mercados financeiros. Griffith-Jones (2010) e Acharya *et. al.* (2009)⁵³, por exemplo, argumentam que a regulação de tais mercados traz ganhos aos consumidores ao reduzir o risco sistêmico, evitando crises com amplas consequências para a economia⁵⁴.

Já existem preocupações com a geração de risco sistêmico no mercado de criptoativos, indicando que tais ganhos regulatórios também poderiam ser notados. Especificamente nesse ponto a classe de ativos que mais preocupa é a das *stablecoins*, já que sua estabilidade permitiria a consumidores entendê-la como ativo de reserva absoluta de valor, ainda que não exista lastro nem garantias em caso de perda da paridade⁵⁵. Com isso, empresas e indivíduos poderiam passar a utilizar ativos dessa classe como parte da operação de seus negócios ou de suas reservas. Nesse cenário, em caso de perda de paridade haveria também um risco de impactos negativos em cascata na economia.

Ainda para o mercado de criptoativos, a literatura aponta que parte significativa do benefício poderia vir da redução da assimetria de informação entre compradores e

⁵³ ACHARYA, Viral V. et al. *Regulating systemic risk. Restoring financial stability: how to repair a failed system.* Hoboken: Wiley, 2009

⁵⁴ “É de particular importância que os governos utilizem a regulação para evitar a geração de risco sistêmico, de modo a evitar também futuras crises, que podem ser profundamente negativas para a economia real.[...] Está cada vez mais claro que uma regulação eficiente não é importante apenas para a economia real, mas também protege a estabilidade do próprio sistema financeiro e as instituições financeiras individuais.” Griffith-Jones (2010, pg. 106)

⁵⁵ “Uma das principais preocupações entre os formuladores de políticas é que o colapso de uma grande *stablecoin* lastreada em ativos possa desencadear vendas de pânico de instrumentos financeiros tradicionais pelos quais eles têm lastro, como *commercial papers*.” Disponível em: <https://valor.globo.com/financas/criptomoedas/noticia/2022/07/11/banco-central-europeu-ve-risco-com-stablecoins-e-pede-urgencia-na-regulacao.ghtml> Acesso em: 08/09/2022.

vendedores, garantindo maior segurança aos usuários, em especial os ingressantes. De acordo com o BIS (Bank for International Settlements, ou Banco de Compensações Internacionais) é importante que exista divulgação dos riscos envolvidos no processo de investimentos em criptoativos, o que implica na necessidade de regulação robusta de propagandas de *exchanges*, que por vezes podem minimizar os riscos envolvidos⁵⁶. Esse tratamento é extremamente prejudicial a consumidores e ao setor como um todo, uma vez que gera incertezas potencialmente descabidas quanto aos criptoativos negociados.

Conforme apresentado na seção 2 há também uma problemática envolvendo presença de *exchanges* em paraísos fiscais. Embora esse problema não se restrinja ao Brasil, a regulação nacional tem espaço para aprimoramentos no combate a ele, dado que é um fenômeno derivado de uma prática que não é ilegal, mas promove assimetria concorrencial. Algumas *exchanges*, por estarem situadas em paraísos fiscais, podem operar em outros países sem estarem sujeitas aos mesmos parâmetros regulatórios que as registradas nesses locais. Isso implica em vantagens significativas no que diz respeito a determinados custos, especialmente tributários.

As vantagens competitivas auferidas em âmbito tributário pelas *exchanges* sem domicílio fiscal no país de operação são objeto de um amplo debate regulatório. Nesse sentido, destaca-se a indicação da OCDE em favor da tributação por presença econômica relevante⁵⁷. Com isso, espera-se que seja possível coibir práticas de *profit shifting*⁵⁸ ou de transações trianguladas, o que mitigaria o problema de empresas domiciliadas em paraísos fiscais, incluindo *exchanges* de criptoativos. Conforme mencionado anteriormente outra possível solução é a posta em prática pelos EUA, que estabeleceu a necessidade da existência de sedes locais para operação no país.

⁵⁶ “While investors should be allowed to invest in risky assets, including cryptocurrencies, there should be adequate disclosure. This implies sound regulation of digital asset advertising by crypto platforms, which can often be misleading and downplay risks.” (BIS, 2022 pg. 88) Tradução livre dos autores.

⁵⁷ A partir desse conceito, fundamenta-se a tributação de *exchanges* estrangeiras e parcialmente nacionalizadas que ultrapassem determinado limite inerente às suas operações no país.

⁵⁸ As práticas de *profit shifting* são definidas como a transferência de lucros entre empresas relacionadas, sendo esses lucros direcionados de um país com maior incidência tributária para outro com impostos reduzidos.

4.1 Panorama regulatório internacional

Dada a incipiência da criptoeconomia e o fato de que a tecnologia blockchain utilizada também é recente, existem grandes desafios ao desenvolvimento de um arcabouço de boas práticas regulatórias para a criptoeconomia. Tal característica permite que a legislação brasileira se aproveite de diferentes aspectos das normas de diferentes jurisdições, mesmo que se preze por uma relativa uniformidade e cooperação regulatória internacional. Como apontado pelo BIS: “*Em todos os temas regulatórios, a natureza global da criptoeconomia e das DeFi requisitará cooperação internacional*”⁵⁹.

Organismos multilaterais versam sobre a urgência de se estabelecer um arcabouço internacional para regulação e tributação de criptoativos, especialmente considerando o caráter transnacional de suas operações. Em abril de 2022, a OCDE publicou o padrão internacional para declaração de operações com criptoativos, denominado CARF (*Crypto-Asset Reporting Framework*)⁶⁰, normatizando as diretrizes já existentes e aumentando o escopo de atuação das autoridades tributárias, já considerando os diversos tipos de intermediários, como *exchanges*, operadores de carteiras, entre outros.

A presente subseção visa apresentar arcabouços que estão sendo desenvolvidos em jurisdições selecionadas, relacionando-os com as normas preexistentes no Brasil e com o principal marco regulatório em discussão no Congresso Nacional, por meio do PL 4.401/2021, apresentado à frente.

4.1.1 Estados Unidos

Atualmente a operação de *exchanges* de criptoativos é legal no país, devendo se conformar ao *Bank Secrecy Act* (BSA)⁶¹ através da submissão de relatórios às

⁵⁹ “*Across all areas of regulation, the global nature of crypto and DeFi will require international cooperation*” (BIS, 2022 pg 88). Disponível em: https://www.bis.org/publ/arpdf/ar2022e.pdf?utm_source=substack&utm_medium=email (acesso em 14/09/2022)

⁶⁰ Disponível em: <https://www.oecd.org/tax/exchange-of-tax-information/public-consultation-document-crypto-asset-reporting-framework-and-amendments-to-the-common-reporting-standard.pdf> (acesso em 14/09/2022).

⁶¹ O BSA instituiu as primeiras leis americanas que visam combater lavagem de dinheiro. A regra requer que empresas mantenham registro e submetam relatórios de um grupo de atividades.

autoridades. Após novembro de 2021, *exchanges* passaram a ser consideradas corretoras, informando o órgão de Receita sobre as operações com criptoativos⁶².

No final de 2021 o *Federal Reserve* (FED), o *Federal Deposit Insurance Corporation* (FDIC) e o *Office of the Comptroller of the Currency* (OCC)⁶³ divulgaram um documento chamado *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps*⁶⁴ que reconhece que a criptoeconomia pertence ao sistema financeiro e reforça sua importância regulatória. Foram divulgados também atividades específicas que requerem atenção dos órgãos, como custódia e empréstimos de criptoativos. Mais recentemente, em março de 2022, a Casa Branca estabeleceu diretrizes para a CBDC americana, bem como definições para “ativos digitais” e “criptomoedas”⁶⁵.

Quanto a propostas específicas para estabelecer regras para o setor, destaca-se sobretudo a *Lummis-Gillibrand Crypto Bill*⁶⁶. O projeto tem como finalidade promover a inovação da tecnologia blockchain e dos seus produtos de forma concomitante à garantia de uma proteção dos consumidores. Utiliza-se como mecanismo regulatório a segmentação da competência de regular criptoativos para órgãos que já possuam o *know-how* por regular bens semelhantes. Dessa forma:

- O *Commodity Futures Trading Commission* (CFTC), que regula commodities, ficaria responsável por *tokens* descentralizados parecidos com esse tipo de ativos, como Bitcoin ou a rede Ethereum⁶⁷.
- Ao FDIC, que regula o sistema bancário, caberia regular as *stablecoins*.

⁶² O movimento foi resultado de uma redefinição da atividade legal de corretoras, que passam a incluir a operações que envolvam ativos digitais. A alteração foi feita no contexto do *Infrastructure Investment and Jobs Act*, dentro do título VI (outras provisões). Fonte: <https://www.congress.gov/bill/117th-congress/house-bill/3684> (acesso em 14/09/2022).

⁶³ O *Federal Reserve*, ou FED, é autoridade responsável pela política monetária americana. O *Federal Deposit Insurance Corporation*, ou FDIC, é uma agência americana independente cuja função é a manutenção da confiança do sistema financeiro. O *Office of the Comptroller of the Currency*, ou OCC, é uma agência americana independente e pertencente ao tesouro nacional, seu objetivo é regular e supervisionar os bancos que operam em solo americano.

⁶⁴ Disponível em: <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf> (acesso em 30/08/2022).

⁶⁵ Disponível em: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/fact-sheet-president-biden-to-sign-executive-order-on-ensuring-responsible-innovation-in-digital-assets/> (acesso em 08/09/2022).

⁶⁶ Disponível em: <https://www.congress.gov/bill/117th-congress/senate-bill/4356/text> (acesso em 30/08/2022).

⁶⁷ Tais ativos são denominados *Bitcoin-like Crypto Assets* (BLCA) de acordo com definição do FMI.

- Por fim a *Securities and Exchange Commission* (SEC), que regula *securities*, supervisionaria tokens de capitalização, como *utility tokens*.

4.1.2 União Europeia

Atualmente, *exchanges* de criptoativos são reguladas por diretrizes de cada Estado-membro, além de atender ao *compliance* das autoridades financeiras europeias. Entretanto, de modo a uniformizar os tratamentos, o bloco caminha para o estabelecimento de normas gerais, inicialmente através da regulamentação da tecnologia DLT, via o *DLT Pilot Regime*⁶⁸, aprovado em junho de 2022, e do mercado de criptoativos, através da *MiCA (Regulation on Markets in Crypto-assets)*⁶⁹.

A *MiCA* é a legislação mais avançada que versa sobre o tópico. A expectativa é que o texto cubra gaps regulatórios importantes, incluindo emissão, custódia e troca de criptoativos (exceto NFT). A partir das normas estabelecidas por esse documento regulatório, provedores de serviços precisariam de autorização para operar na União Europeia e devem se responsabilizar pelos ativos de seus clientes. Haveria também a necessidade de que todas as *stablecoins* possuam reservas líquidas robustas e limitações em valor transacionado diário, condições que serão fiscalizadas pela autoridade bancária (*European Banking Authority*, ou EBA). Há, também dentro da legislação proposta, espaço para que a autoridade de investimentos (*European Securities and Markets Authority*, ou ESMA) desenvolva padrões técnicos para avaliar impacto ambiental dos ativos.

Cabe ressaltar que países asiáticos, como Japão e Singapura, têm seguido tais diretrizes estabelecidas pela União Europeia⁷⁰, sobretudo por esta possuir o debate mais avançado dentre as legislações discutidas em países desenvolvidos. Se comparada à legislação proposta nos EUA, é notória a concordância na segmentação regulatória entre agências governamentais já existentes. Especificamente o destaque dado às *stablecoins* é digno de atenção, visto que em ambos os casos as moedas

⁶⁸ O *DLT Pilot Regime* é uma proposta de regulamentação que tem como objetivo fornecer um aparato legal para a infraestrutura de mercado de DLT. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0594> (acesso em 30/08/2022)

⁶⁸ Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593> (acesso em 30/08/2022).

⁶⁹ Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593> (acesso em 30/08/2022).

⁷⁰ Segundo apresentação institucional do Banco Central do Brasil.

lastreadas tem classificação distinta e designação exclusiva para os respectivos órgãos reguladores bancários. Por outro lado, a União Europeia não aprofunda tal classificação de ativos, como faz a proposta americana, que diferencia o restante dos *tokens* entre commodities e valores mobiliários⁷¹.

Box 4: Panorama geral e outras jurisdições

Para além das jurisdições apresentadas, ressalta-se que o processo de regulação de criptoativos é uma tendência no mundo todo, com crescimento expressivo de normas aprovadas nos últimos anos. Um relatório do Congresso Americano, que avaliou 130 países em junho de 2018 e em novembro de 2021, encontrou que na primeira data somente 33 países apresentavam algum tipo de legislação para regulação de criptoativos, envolvendo tributação e/ou prevenção de lavagem de dinheiro e financiamento de terrorismo. Para o período mais recente, observou-se que havia aumentado para 103 o número de países que apresentam algumas destas legislações⁷², aproximadamente 77% da amostra.

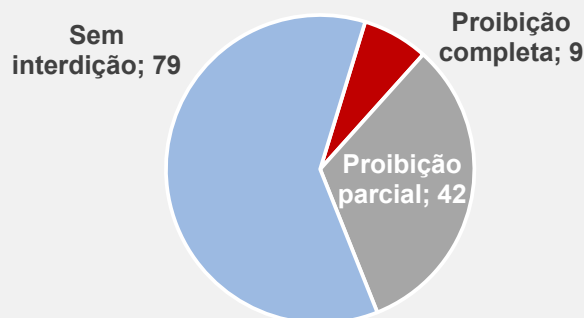
O Gráfico 11 apresenta a posição dos mesmos 130 países quanto a proibição de criptoativos em 2021. Nota-se que não há interdição na maior parte destes, enquanto 42 países apresentam proibições parciais em criptoativos, como impedir uso destes como meio de pagamento (Turquia) ou interditar operação de *exchanges* e aquisição por instituições financeiras (Bolívia). Criptoativos são inteiramente banidos em 9 países, incluindo a China⁷³.

⁷¹ Há de se observar que a ausência de tal distinção no contexto europeu não se deve à falta de desenvolvimento regulatório e sim a ausência de órgãos específicos para cada um dos ativos. No caso brasileiro também não há essa diferença, ambos são regulados pela Comissão de Valores Mobiliários (CVM).

⁷² Geralmente os países apresentam ambas as legislações e possuem forte influência das normas europeias implementadas em 2020.

⁷³ Exceto yuan digital, CBDC em desenvolvimento.

Gráfico 11: Proibição de criptoativos pelo mundo, em 2021



Fonte: *The Law Library of Congress (2021). Regulation of Cryptocurrency Around the World: November 2021 Update. Elaboração: LCA Consultores.*

Para além desse panorama, outras jurisdições possuem temas relevantes com regulação avançada, dentre as quais destaca-se:

- Japão: a legislação japonesa sobre criptoativos é considerada uma das mais avançadas no mundo. As criptomoedas são tratadas como propriedades legais, e o funcionamento dos mercados de criptoativos é amparado pelo *Payment Services Act (PSA)*. A regulação autoriza apenas operações de *exchanges* de criptoativos que possuam um escritório financeiro no país, ou que demonstrem um padrão de registro equivalente em seu país-sede⁷⁴.
- Suíça: no país, os criptoativos são considerados como ativos ou propriedades. Isso faz com que os ganhos de capital, renda e patrimônio derivados de operações com criptoativos sejam tributados sob a regulamentação da *Swiss Federal Tax Administration (SFTA)*. As *exchanges* precisam de autorização para operar no país, e o fazem a partir de licença concedida pela *Swiss Financial Market Supervisory Authority (FINMA)*⁷⁵.

4.2 Regulação no Brasil

No Brasil a regulação de ativos financeiros segue uma divisão de competências de acordo com categorias específicas de ativos. Dentre tais segmentos é possível destacar

⁷⁴ Fonte: <https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-japan/>. Acesso em: 16/09/2022.

⁷⁵ Fonte: <https://complyadvantage.com/insights/crypto-regulations/cryptocurrency-regulations-switzerland/>. Acesso em: 16/09/2022.

três: os valores mobiliários, as moedas eletrônicas e, mais recentemente, os ativos virtuais, dentre os quais se inserem os criptoativos⁷⁶.

A regulação dos mercados de títulos mobiliários⁷⁷ é competência de dois órgãos: a Comissão de Valores Mobiliários (CVM) e o Conselho Monetário Nacional (CMN), cujas atribuições são definidas pela Lei nº 6.385/1976. Esta destaca algumas funções a serem desempenhadas pelas instituições reguladoras, tais como a promoção da eficiência do mercado de ações e a proteção dos titulares de valores mobiliários. Com relação às moedas eletrônicas⁷⁸, tem-se o Banco Central⁷⁹ como órgão regulador de tais mercados, que constituem arranjos de pagamento digitais. A competência do Banco Central é atribuída pela Lei nº 12.865/2013, que integra os arranjos de pagamento digitais ao Sistema de Pagamentos Brasileiro (SPB), cuja regulação já cabe ao BCB.

Os ativos virtuais, por sua vez, ainda não possuem um arcabouço regulatório específico e por isso são objeto do Projeto de Lei (PL) nº 4.401/2021, ainda em discussão no Congresso Nacional. A regulação de tais mercados, apesar de ainda não consolidada, já possui algumas normas estabelecidas. As subseções a seguir analisarão as medidas que regulam de ativos virtuais no Brasil atualmente e a referida proposta de legislação.

4.2.1 Histórico regulatório

Como apontado, a ausência de uma legislação específica para criptoativos faz com que as normas que regulam a atividade partam de diversos órgãos nacionais. Até o presente momento há manifestações do BCB, da CVM e da RFB sobre o tema. Tais deliberações estabelecem definições importantes e algumas regras para o setor e seus participantes.

⁷⁶ O termo “ativos virtuais” é tratado como referência legal para criptoativos. Ainda que ele não esteja restrito ao universo cripto, parte dos produtos da criptoeconomia não são englobados por ele, de acordo com a definição proposta no PL 4.401/2021. Essa distinção será mais bem explorada durante a apresentação da proposta.

⁷⁷ Valores Mobiliários podem ser definidos como títulos ou contratos de investimento ofertados publicamente, que gerem direito de participação dos quais os rendimentos advêm de esforços do empreendedor.

⁷⁸ Define-se como recursos armazenados em dispositivo ou sistema eletrônico, que permitem ao usuário efetuar transações de pagamento. As moedas eletrônicas são partes de arranjos de pagamento digitais.

⁷⁹ As diretrizes para a atuação do BCB são também atribuídas pelo CMN. No tocante à regulação dos arranjos de pagamento digitais, cabe ao Banco Central disciplinar, fiscalizar e limitar o objeto social de instituições de pagamento, além de assegurar solidez e eficiência de arranjos de pagamento.

A Figura 4 resume as principais deliberações dos últimos anos, que por consequência formam o atual arcabouço regulatório do mercado.

Figura 4: Deliberações de órgãos governamentais a respeito de criptoativos



Fonte: Sítios Eletrônicos do Banco Central do Brasil. Comissão de Valores Mobiliários e Receita Federal do Brasil. Elaboração: LCA Consultores

Destaca-se, em especial, a importante diferenciação feita pelo BCB em 2014 entre moedas eletrônicas e virtuais, de forma a excluir os criptoativos da já mencionada legislação de moedas eletrônicas. A diferenciação ou equiparação de criptoativos a ativos financeiros também se apresenta como tema importante e que necessita de pacificação, sobretudo dado o seu entendimento difuso entre as manifestações dos órgãos.

4.2.2 Projeto de lei em discussão no Brasil: PL 4.401/2021

Com o intuito de criar um arcabouço específico para os criptoativos e agentes da criptoeconomia, desde 2015 são formulados projetos de lei para ativos virtuais. Em 2021, o Projeto de Lei 4.401/2021, de iniciativa do Deputado Federal Aureo Ribeiro (SOLIDARIEDADE/RJ), integrou proposições dos antigos projetos e desenvolveu novos pontos a fim de criar uma proposta única e madura de regulação para o setor. Serão resumidos nesta subseção alguns dos principais pontos propostos no texto e em suas emendas.

O projeto define ativos virtuais como representação digital de valor que pode ser negociada por meios eletrônicos e utilizada para pagamentos ou investimentos, excetuando apenas: valores mobiliários, moedas (inclusive eletrônicas), instrumentos que provejam acesso a produtos ou serviços especificados e representações de ativos financeiros já regulados. Por essa definição NFTs e *utility* tokens⁸⁰ não seriam considerados ativos virtuais, de forma que não seriam regulados pela lei caso aprovada, necessitando de ato posterior.

Já as prestadoras de serviços de ativos virtuais são definidas como as pessoas jurídicas que executam, para terceiros, pelo menos um dos serviços de ativos virtuais:

- Troca entre ativos virtuais e moeda, entre um ou mais ativos virtuais ou transferência;
- Custódia ou administração;
- Participação em serviços financeiros e prestação de serviços relacionados à oferta por um emissor ou venda.

A regulamentação das *exchanges* como prestadoras de serviços garante os mecanismos jurídicos que permitem maior informação, transparência e proteção do investidor contra eventuais assimetrias, fraudes, bem como protege os dados dos consumidores de serviços de *exchanges*. Além disso, o enquadramento facilita o monitoramento do mercado, o que trabalha em favor da prevenção e gestão de riscos ligados a estabilidade do mercado.

⁸⁰ Ambos os ativos podem ser enquadrados como “instrumentos que provejam acesso a produtos ou serviços especificados”, excetuados da definição de ativos virtuais.

Quanto ao órgão responsável pela supervisão das *exchanges*, propõe-se que este seja definido posteriormente pelo Executivo. A autoridade teria como competência autorizar e suspender funcionamento de prestadoras de serviços de ativos digitais que não se conformem a diretrizes estabelecidas.

Por fim, o projeto também prevê que a Lei de Crimes Financeiros (nº 7.492/1986) passe a prever a necessidade de autorização prévia para a prestação de serviços ligados a ativos virtuais. Essa obrigação dificulta a operação de *exchanges* não domiciliadas no país uma vez que considera crime emitir, oferecer ou negociar tais ativos com a ausência da autorização prévia da autoridade competente⁸¹.

Do panorama regulatório apresentado cabe destacar:

- Não há consenso sobre quais seriam as boas práticas regulatórias que deveriam ser estabelecidas para garantir maior eficiência aos mercados;
- Cooperação internacional e análise comparativa de legislações podem contribuir para a construção do arcabouço legal para operações de criptoativos no Brasil;
- Legislação proposta nos EUA e legislação europeia alinham-se acerca da importância de diferenciar *stablecoins* dos demais criptoativos, entregando a competência de regulá-las ao órgão responsável pelo sistema bancário. Os demais ativos são tratados como valores mobiliários e/ou commodities;
- Brasil possui normas pouco abrangentes e pouco objetivas para o setor;
- Principal proposta de lei está em discussão no congresso nacional na forma do PL 4.401/2021. O projeto estabelece definições importantes e confere ao executivo o poder de definir a autoridade que regulará o funcionamento da criptoeconomia. No entanto, o projeto deixa de fora algumas classes de ativos.

⁸¹ Nesse caso a pena varia de é de reclusão de 2 a 8 anos além de multa (artigo 7º, inciso quarto da Lei supracitada).

5. Tributação de *exchanges* de criptoativos no Brasil

Dentre as práticas regulatórias ainda a serem mais bem definidas, aquelas relativas à incidência tributária representam um passo relevante para a formalização do setor. Não há, nem no contexto nacional nem no internacional, um entendimento pacificado acerca dos enquadramentos e incidências tributárias para cada um dos agentes da criptoeconomia. Entretanto, assim como no debate regulatório, existem proposições de órgãos multilaterais e legislações em vigor em outros países e no Brasil. O Box 5, apresentado abaixo, resume alguns dos tratamentos tributários para criptoativos no mundo.

Ainda que o ambiente seja permeado por essas diversas incertezas, atualmente, as *exchanges* que se conformam à regulação já estão sujeitas às obrigações tributárias, dado que constituem pessoa jurídica prestadora de serviços. Ao menos, tal condição implica no recolhimento de tributos indiretos, como PIS/Cofins⁸² e o Imposto Sobre Serviços (ISS), e de alguns tributos diretos sobre a renda corporativa, como o Imposto sobre a Renda das Pessoas Jurídicas (IRPJ) e a Contribuição Social sobre o Lucro Líquido (CSLL). Outras atividades realizadas pelas *exchanges* também são tributáveis de maneiras indiretas, como pela realização de contratos cambiais, fundamental para a atividade de *market-makers* e que resulta na incidência do Imposto sobre Operações Financeiras (IOF).







Para os propósitos desta seção, as *exchanges* que prestam serviços no Brasil são segmentadas em dois grupos: o primeiro, que é contribuinte dos tributos supracitados sobre o faturamento advindo das operações de transação e de saque. Tal grupo é composto pelas empresas classificadas como nacionais e nacionalizadas na Seção 3, que são as *exchanges* cuja estrutura societária indica que possuem a totalidade das suas operações no Brasil e por isso foram consideradas atuais contribuintes de tais tributos. O segundo grupo possivelmente ainda não contribui com a totalidade dos tributos, e incorpora, além das *exchanges* classificadas como estrangeiras na Seção 3,

⁸² PIS/COFINS: termo geralmente usado para representar o conjunto de tributos formado pelo Programa de Integração Social (PIS), Programa de Formação de Patrimônio do Servidor Público (PASEP) e pela Contribuição para o Financiamento da Seguridade Social (COFINS). Na prática, o PIS/PASEP é tratado como uma contribuição única, pois financiam um único fundo.

as empresas parcialmente nacionalizadas, que ainda que tenham parte de suas operações no Brasil, realizam a intermediação de criptoativos através de associados no exterior. Entende-se que esse grupo, no ano de 2021, não esteve sujeito aos tributos analisados nesta seção e só estariam sujeitos em um cenário de internalização, mais bem explicado à frente.

Faz-se relevante, então, estimar, com base no ano de 2021, o recolhimento atual das *exchanges* de criptoativos de tributos sobre receita bruta (PIS/Cofins e ISS), lucro líquido (IRPJ e CSLL) e operações cambiais (IOF)⁸³. Adicionalmente, estima-se também um cenário em que as demais *exchanges* em operação no mercado brasileiro passem a cumprir com as mesmas normas tributárias. A Figura 5 apresenta um breve resumo dos resultados de faturamento e recolhimento tributário das *exchanges* em cada cenário⁸⁴.

Figura 5: Resumo dos resultados

 Exchange	 Faturamento	 Arrecadação
 Quadro atual	R\$ 985 milhões	R\$ 314 milhões
 Internalização	Entre R\$ 423 - 719 milhões	Entre R\$ 193 - 247 milhões
 Total	Entre R\$ 1,4 - 1,7 bilhões	Entre R\$ 507 - 561 milhões

Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA Consultores.

⁸³ Cabe ressaltar que tal estimativa é parcial, uma vez que há arrecadação de outros tributos ligados ao setor (IRPF, recolhimento sobre a folha de pagamentos, aquisição de insumos etc.). Há também potencial arrecadatório em diversos agentes e operações não tratados neste estudo (apresentados de maneira detalhada mais à frente).

⁸⁴ Como apontado na seção 2, que o escopo desse trabalho engloba apenas algumas atividades e operadores da criptoeconomia sobretudo pela falta de dados relativos ao faturamento de outros agentes e operações.

Box 5: Tributação de criptoativos no mundo – referência OCDE (2020)

Em 2020, a OCDE publicou um artigo preparado e endossado pelos membros do grupo de colaboração para combate à evasão tributária (BEPS) apresentando um panorama dos tratamentos e políticas tributárias para a criptoeconomia em mais de 50 jurisdições.

Segundo o relatório, para os fins de tributação sobre ganhos de capital em geral criptoativos são considerados uma forma de propriedade. Esse tratamento, no entanto, não é um consenso. Algumas jurisdições ao redor do mundo adotam outros tipos de abordagens em relação ao tratamento regulatório de criptoativos, dentre as quais se destacam as definições:

- francesa, que classifica como ativos intangíveis;
- austríaca, como mercadorias;
- japonesa como instrumentos/ativos financeiros e;
- italiana, como moeda estrangeira.

Quanto à definição para fins de tributação sobre consumo, considera-se usualmente que as trocas entre criptoativos ou entre criptoativos e moedas fiduciárias não geram valor adicionado para propósitos de tributação, especificamente quando realizadas sem a prestação de serviços de um intermediário, seguindo a decisão de Heqdvist na União Europeia. Quando há a prestação de serviços por exchanges, a intermediação de criptoativos é tipicamente considerada passível de incidência de Imposto de Valor Adicionado (IVA). Isso confere às plataformas de intermediação de ativos virtuais um tratamento equivalente ao de intermediadoras financeiras. O IVA, porém, não é cobrado em muitos países, especialmente na União Europeia, em decorrência da isenção concedida a demais serviços financeiros.

O relatório da OCDE também versa sobre tributação de outras atividades da criptoeconomia, tendo em vista o processo de diversificação de tipos de ativos e suas respectivas funcionalidades práticas. Há, entretanto, poucas concordâncias entre os países da organização acerca de qual seria a incidência tributária ideal, considerando-se as especificidades de cada atividade. Destaca-se como tributáveis, sobretudo, os negócios relacionados à mineração e ao armazenamento, ainda que não exista nenhum alinhamento entre os tratamentos tributários dos países em relação a eles.

5.1 Estimativa da tributação atual

Nesta subseção serão apresentadas as estimativas de arrecadação atual de *exchanges* nacionais e nacionalizadas de criptoativos, grupos que tem a totalidade de suas atividades domiciliadas no Brasil e, portanto, entende-se que a todas as suas operações são tributáveis. Para este propósito é necessário estimar o faturamento de tais *exchanges* e, em seguida, presumir incidências tributárias de forma a calcular o potencial de arrecadação do setor. A Figura 6 apresenta o passo-a-passo de todo o processo. De forma resumida, ele pode ser segmentado em:

- Dimensionamento do mercado, apresentado na seção 3;
- Estimativa de faturamento por meio de taxas médias, que será exposto na subseção 5.2.1 a seguir (resumidamente explicado pelo ponto 1 da figura);
- Aplicação de tributos sobre faturamento das *exchanges* e sobre importação de criptomoedas, processo explicado na subseção 5.2.2. (resumidamente explicado pelos pontos 2 e 3 da figura).

Figura 6: Passo-a-passo da estimativa tributária

Estimativa de arrecadação potencial de *exchanges* de criptoativos

1. Dado o dimensionamento do mercado – em termos de transação, apresentado na seção 3, e de saques apresentado no Box 6 desta seção – estima-se o faturamento tributável atual das *exchanges* a partir da aplicação das taxas cobradas:
 - Taxa de **ordem**, cobrada como % do valor da transacionado
 - Taxa de **saque**: valor fixo por saque (doravante taxa fixa) e/ou % sobre valor sacado (doravante taxa variável)

Obs: Exchanges possuem outras fontes de receita, não incluídas nesta estimativa por não constarem em bases de dados públicas.
2. Sobre o faturamento são aplicadas as alíquotas dos tributos sobre prestação de serviços e sobre renda corporativa
 - Supõe-se que 100% das *exchanges* nacionais identificadas contribuem para o fisco. Para as *exchanges* estrangeiras e parcialmente nacionalizadas serão apresentados outros cenários.
3. Adicionalmente, estima-se a arrecadação sobre operações cambiais, através dos dados de importações de criptoativos (BCB)

Elaboração: LCA Consultores.

O cálculo da receita das empresas foi realizado considerando duas atividades fundamentais exercidas por essas plataformas: intermediação e saques. Reconhece-se que, para além destas, existem outras fontes de faturamento não incluídas por não constarem em bases de dados públicas. Vale pontuar que também existem outras possibilidades de incidência tributária, por se esperar que exista arrecadação de outros tributos ligados ao setor, como por exemplo de Imposto de Renda sobre Pessoas Físicas (IRPF), e tributos sobre a folha de pagamentos, entre outros. Por ambos os motivos, a estimativa apresentada a seguir não abrange o conjunto completo de arrecadação potencial das *exchanges*.

Para além disso, há um potencial arrecadatário em diversos outros agentes e operações não tratados neste estudo já que as suas incidências tributárias contam com definições ainda menos claras na legislação, de modo que há espaço para discussões relativas a interpretações das regras tributárias⁸⁵. Dentre alguns desses pontos em discussão, pode-se apontar as seguintes possibilidades de incidência tributária para os agentes e operações indicados:

- Tokenizadoras: Incidência de ISS ou de ICMS, e tributos sobre renda;
- OTCs e Custodiantes: Incidência de ISS e tributos sobre renda corporativa;

No Brasil, especialmente as atividades com *tokens* trazem consigo dúvidas relevantes da forma como pode se dar sua tributação. Esse é um processo complexo e ainda incipiente. Algumas possibilidades relativas à tributação de *tokens* podem ser apresentadas a título de exemplo, como a incidência de ICMS sobre a posse e emissão de ativos tokenizados, incidência de IOF sobre a tokenização de debêntures, e incidência de PIS/Cofins e ISS sobre a prestação de serviços de tokenização.

5.1.1 Estimativa do faturamento tributável das *exchanges* nacionais e nacionalizadas

Seguindo o passo-a-passo apresentado, para computar o faturamento das *exchanges* nacionais e nacionalizadas foram aplicadas as taxas médias sobre os mercados dimensionados. As equações abaixo mostram como foram computadas as receitas:

$$Receita_{ordem} = taxa_{média_{ordem}} * transações_{exchanges_{br}}$$

⁸⁵ Tais discussões fazem com que, na maior parte dos casos, ainda não exista um recolhimento padronizado por tais empresas e/ou operações.

$$Receita_{saque} = taxa_{m\u00e9dia_{saque}} * saques_{exchanges_{br}}$$

As taxas utilizadas foram compiladas pelo agregador *CoinTrade Monitor*⁸⁶ a partir de informações coletadas junto a cada *exchange*, em maio/2022⁸⁷. Para as *exchanges* que são atualmente contribuintes destes tributos, a média ponderada⁸⁸ da taxa de ordem (*taker*) foi de 0,43% em 2021. No caso das taxas de saque, as médias ponderadas pelo mesmo fator resultam em valor fixo de R\$ 5 e variável de 0,40%, cobrados a cada retirada de recursos. A Tabela 3 apresenta os resultados encontrados, além de ressaltar o mercado de ordem, dimensionado na seção 3, e as taxas utilizadas no cálculo. A quantidade e o volume de saques foram dimensionados de acordo com a metodologia apresentada no Box 6.

Tabela 3: Estimativa de faturamento das *exchanges*, em R\$ milhões, em 2021

Variável	Ordem	Saques	Total
Valor (ordem e saque) (A)	R\$ 183.552,50	R\$ 48.922,50	R\$ 232.475,00
Número de saques (B)	-	222.716	
Taxas médias (C)	0,43%	0,40% e R\$ 5,00	
Faturamento das <i>exchanges</i> (A*C + B*C)	R\$ 787,30	R\$ 196,90 + R\$ 1,1 = R\$ 198,00	R\$ 985,30

Nota: O número de saques não segue a unidade de medida da tabela e está expresso em unidades. Fonte: *CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA: Consultores.*

Para a realização da estimativa de arrecadação é importante supor que o faturamento calculado é bruto, ou seja, já contém os tributos sobre consumo calculados⁸⁹. Essas premissas são relevantes para as hipóteses de incidência assumidas, conforme será explicitado abaixo.

⁸⁶ <https://cointradermonitor.com/taxas-exchanges> . Acesso em maio de 2022.

⁸⁷ O Anexo 2 apresenta todas as taxas utilizadas no cálculo, bem como o *market share* das *exchanges* no período.

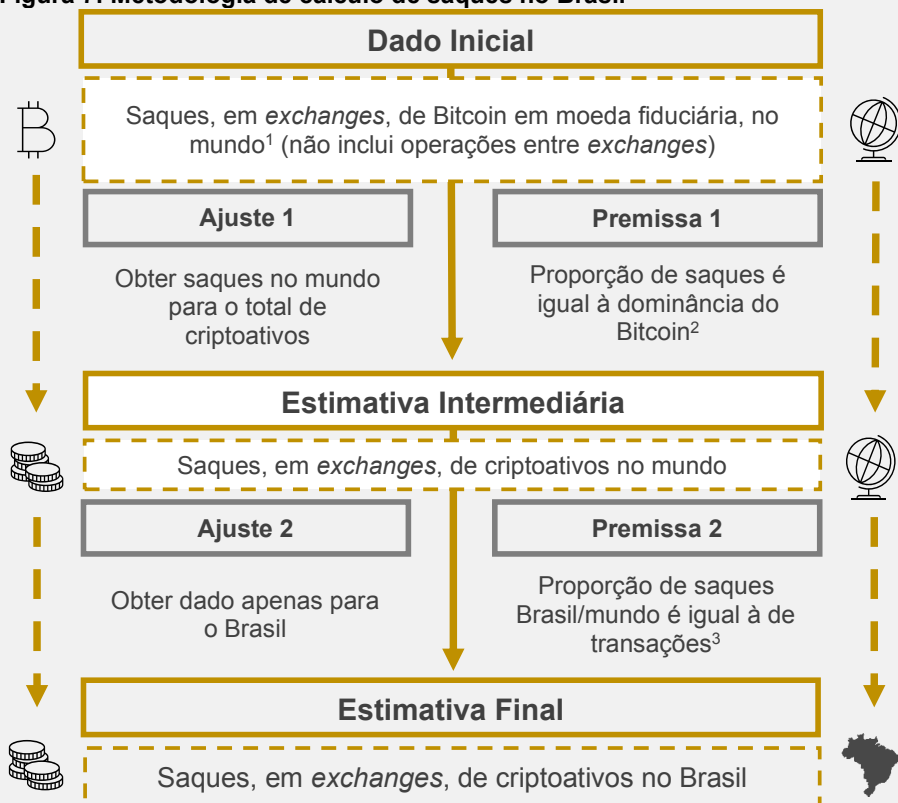
⁸⁸ A ponderação foi realizada através dos dados de *market share* das empresas no ano de referência.

⁸⁹ As *exchanges* nacionais incluem em suas taxas os tributos pagos, de forma que o faturamento estimado já compreende o recolhimento tributário.

Box 6: Metodologia de estimativa do mercado saques no Brasil

A metodologia para cálculo de número e valor sacado em *exchanges* no Brasil requer um novo conjunto de premissas⁹⁰. Tais informações, bem como os ajustes necessários, fontes e os dados utilizados estão resumidos na Figura 7.

Figura 7: Metodologia de cálculo de saques no Brasil



Notas: 1. Dados em número de saques e valor total sacado. Fonte: CoinMetrics. 2. Dado de proporção de valor BTC/Total de criptoativos. Retirado de Messari.io. 3. Dado de transações em *exchanges* no Brasil estimado nesse mesmo estudo. Dado de transações mundiais em *exchanges* extraído do agregador Bitcoinity. Elaboração: LCA Consultores.

Através dessa metodologia, para 2021, estimou-se um total de 380.490 saques em *exchanges* no Brasil, com valor total de R\$ 85 bilhões. Desta cifra, R\$ 36,7 bi foram sacados através de *exchanges* nacionais, R\$ 12,2 bi de nacionalizadas, R\$ 7,9 bi de parcialmente nacionalizadas e R\$ 28,1 bi por meio de estrangeiras, como resume a Tabela 4.

Tabela 4: Saques de criptoativos em reais em exchanges, por divisão entre classificação de domicílio fiscal, em 2021

<i>Exchange</i>	Nº de saques	Volume (milhões)	
Estrangeira	123.816	R\$	28.124
Parcialmente Nacionalizada	33.957	R\$	7.891
Nacionalizada	55.523	R\$	12.254
Nacional	167.193	R\$	36.668
Total	380.490	R\$	84.937

Fontes: CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA Consultores.

5.1.2 Cálculo da arrecadação tributária

Conforme apresentado na metodologia descrita acima, sobre o faturamento estimado incidem tributos sobre prestação de serviços e renda corporativa. A Tabela 5 apresenta características gerais dos tributos utilizados na análise e as premissas assumidas para realização do cálculo supracitado.

⁹⁰ A fonte define saques como a soma das transferências que partiram de uma *exchange* e não tiveram uma *exchange* (a mesma ou outra) como destino. Existem informações relativas à contagem de transferências deste tipo e ao volume transacionado nelas. De acordo com o site (Coinmetrics): “this metric applies the following logic: If the input addresses belong to X, then only the outputs where the address doesn’t belong to any exchange are counted as transfers from X. For account-based protocols, if both sender and recipient belong to an exchange, the transfer is not counted”. Quanto ao dado em valor, segundo o site esse se refere a: “The sum USD value withdrawn from exchanges that day, excluding exchange to exchange activity”. Disponível em: <https://docs.coinmetrics.io/asset-metrics/exchange/flowtfrfromexcnt> e <https://docs.coinmetrics.io/asset-metrics/exchange/flowoutexUSD> (acesso em 14/09/2022).

Tabela 5: Características e premissas dos tributos considerados na análise

Tributo	PIS/Cofins	ISS	IRPJ e CSLL
Competência	Federal	Municipal	Federal
Incidência	Bens e serviços prestados por pessoa jurídica	Prestação de serviços	Renda auferida por pessoas jurídicas
Premissas	<p>PIS/Cofins e ISS possuem como base a receita bruta (incluindo os próprios produtos - cálculo "por dentro"). Embora as bases de cálculo de ISS e de PIS/Cofins não sejam idênticas, por simplificação as alíquotas dos tributos foram aplicadas sobre o mesmo valor.</p> <p>Por simplicidade, adotou-se uma alíquota de PIS/Cofins cumulativa, observada pelas empresas de lucro presumido</p> <p>Considera-se que tal alíquota pode ser uma estimativa conservadora da arrecadação para empresas que porventura estariam no Lucro Real e operariam sobre a incidência não cumulativa</p>		<p>Considerando a grande variabilidade da rentabilidade das empresas do lucro real, assume-se por simplificação a regra de tributação sobre empresas do lucro presumido. Deste modo, IRPJ e CSLL incidiriam sobre a receita bruta.</p> <p>Considerou-se a alíquota total de 25% para o IRPJ, considerando que as <i>exchanges</i> tem lucro mensal maior que R\$ 20 mil mensais.</p> <p>Supõe-se que <i>exchanges</i> não se enquadram na categoria de instituições financeiras, de seguros privados e de capitalização, de modo que pagam a alíquota de CSLL de 9%¹.</p>

Nota: 1. Observa-se que para Instituições financeiras e assemelhadas a alíquota de CSLL é de 15%. Dado que as receitas consideradas neste estudo são operacionais e não financeiras as exchanges foram enquadradas fora dessa classificação. Elaboração LCA: Consultores.

A partir de tais premissas foram estabelecidas as bases de incidência e as alíquotas para estimar a arrecadação por tributo e por atividade (ordem e saque). A Tabela 6 destaca a base de incidência calculada, as alíquotas utilizadas e os resultados segmentados.

Tabela 6: Base de incidência, alíquotas e arrecadação tributária estimada para 2021

Tributo	PIS/Cofins	ISS	IRPJ	CSLL
Base de Incidência (A)	R\$ 985.398.190		R\$ 315.327.421	
Alíquota (B)	3,65% ¹	5% ²	25%	9%
Arrecadação – Saques	R\$ 7.228.613	R\$ 9.902.210	R\$ 15.843.536	R\$ 5.703.673
Arrecadação - Ordem	R\$ 28.738.421	R\$ 39.367.699	R\$ 62.988.319	R\$ 22.675.795
Arrecadação – Total (A*B)	R\$ 35.967.034	R\$ 49.269.910	R\$ 78.831.855	R\$ 28.379.468

Nota: Base de incidência de PIS/Cofins e ISS é o faturamento estimado. Para IRPJ e CSLL a base é o lucro tributável estimado, igual ao faturamento vezes 32% (alíquota de presunção para intermediação de negócios). 1. Lei nº 10.833/2003. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/110.833.htm 2. Enquadrada no item 10.01 da Lei Complementar 116/2003, alíquota de 5% válida para o município de São Paulo. Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA: Consultores.

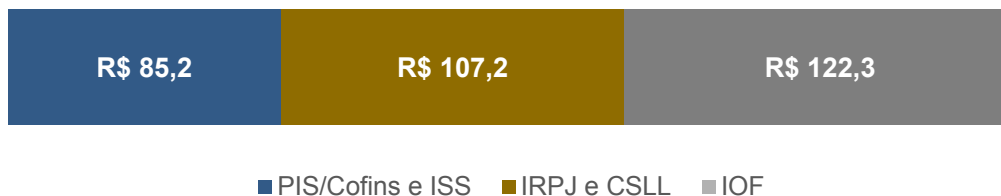
Além desses tributos, há incidência de IOF sobre operações cambiais originárias do processo de importação de criptoativos. Uma vez que a metodologia utilizada pelo BCB utiliza contratos de câmbio para estimar a importação de criptoativos tem-se que o valor de tal fluxo comercial é idêntico ao dos contratos firmados, por definição.

Para os propósitos deste estudo entende-se que incidem sobre contratos cambiais uma alíquota de 0,38% de IOF⁹¹. Como apresentado na Seção 3, para 2021, o BCB calcula que foram importados R\$ 32,2 bilhões de criptoativos, aplicando a alíquota sobre este valor estima-se uma arrecadação de R\$ 122 milhões.

Incluindo então o IOF, a soma dos cinco tributos resulta em uma arrecadação total estimada de R\$ 314,7 milhões, segmentadas conforme apresentado pelo Gráfico 12.

⁹¹ Como transferências internacionais a terceiros, realizadas em moeda estrangeira.

Gráfico 12: Estimativa de arrecadação por incidência tributária, por participação no total estimado, em milhões (2021)



Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcoinity e BCB. Elaboração LCA Consultores.

5.2 Estimativa da tributação potencial das *demais exchanges*

Para além das *exchanges* nacionais, há um potencial de arrecadação dos tributos supracitados na operação de empresas estrangeiras e parcialmente nacionalizadas. No entanto, para que o fisco seja capaz de recolher esse valor, é necessário conjecturar quanto aos possíveis cenários que tornem as *exchanges* estrangeiras e parcialmente nacionalizadas sujeitas à tributação brasileira⁹². Através disso, esta subseção se presta a dimensionar, ainda que preliminarmente, o potencial de arrecadação destas dentro de tais conjunturas. A apresentação destas é necessária uma vez que, embora hoje tais *exchanges* não sejam contribuintes dos tributos sobre as operações consideradas, é possível que em breve exista uma obrigação de regularização através da autorização para operação no Brasil, a ser emitida por órgãos reguladores. Esse é um dos pontos previstos no PL 4.401/2021, por exemplo.

Para os propósitos deste trabalho considera-se que essas empresas poderiam estar sujeitas a recolhimentos do sistema tributário brasileiro de duas formas principais:

1. Criando domicílio fiscal no Brasil – processo doravante chamado de internalização;
2. Mantendo suas sedes domiciliadas no exterior e exportando serviços ao Brasil.

⁹² Sujeição tributária, para estes exercícios, não implicaria necessariamente em conformidade a todos os aspectos regulatórios. Por exemplo, a conformidade a eventuais padrões ambientais estabelecidos na legislação pode ser dificilmente executável quando houver importação de serviços.

Neste trabalho opta-se pela apresentação de estimativas de internalização no corpo do texto; o cenário de sujeição via importação de serviços se encontra no Box 7, apresentado ao final desta seção.

Um fator importante que deve ser considerado na análise é que o pagamento dos tributos supracitados pelas *exchanges* sem domicílio completo poderia levar a taxas mais próximas às cobradas atualmente por aquelas que possuem domicílio fiscal completo no Brasil. Hoje as primeiras têm menores taxas médias de serviços. Estima-se que, na média⁹³, as *exchanges* que não possuem a totalidade de suas atividades domiciliadas no Brasil possuem taxas de ordem e o componente fixo da taxa de saque inferiores às nacionais e nacionalizadas, enquanto o componente variável da taxa de saque se mostra próximo.

Os valores estimados são:

- Taxa de ordem: 0,43% para as nacionais e nacionalizadas X 0,20% para estrangeiras e parcialmente nacionalizadas;
- Taxa de saque: R\$ 5 e 0,40% para nacionais e nacionalizadas X R\$ 3,46 e 0,42% para estrangeiras e parcialmente nacionalizadas⁹⁴.

Visando incorporar o entendimento de que as taxas atualmente cobradas por cada uma das *exchanges* já refletem parcialmente sua sujeição à tributação nacional, foram construídos dois cenários em que as *exchanges* estrangeiras e parcialmente nacionalizada estariam sujeitas às mesmas normas tributárias que as nacionais. Sendo eles:

- Cenário A, que há a manutenção das taxas atuais cobradas pelas *exchanges* estrangeiras e parcialmente nacionalizadas;
- Cenário B, em que as taxas cobradas pelas *exchanges* estrangeiras e parcialmente nacionalizadas são iguais às taxas atuais nacionais e nacionalizadas⁹⁵.

⁹³ A média foi ponderada de acordo com o *market share* de cada *exchange*. Fonte: *CoinTrader monitor*. Vide Anexo 1 para detalhes de *share*, classificação e taxas utilizadas.

⁹⁴ Adotou-se a hipótese de que as taxas cobradas pelas *exchanges* estrangeiras e parcialmente nacionalizadas não incluem os tributos nacionais.

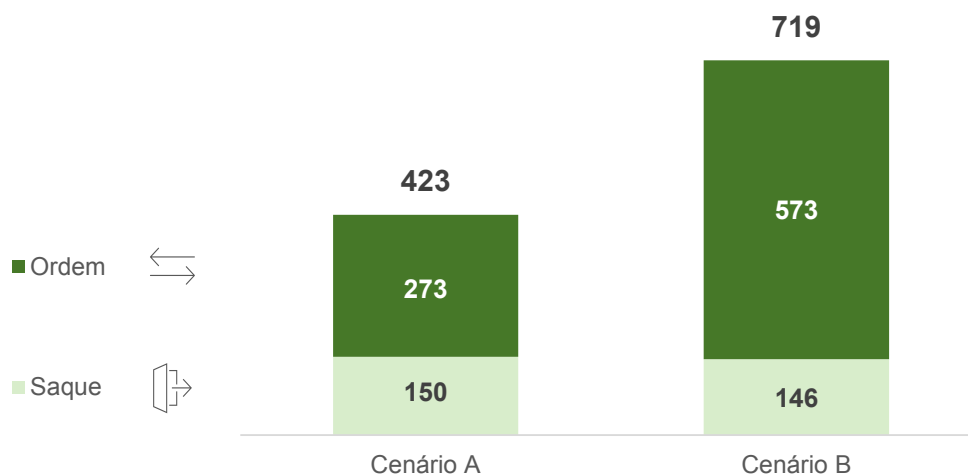
⁹⁵ Taxa de 0,43% para ordem e R\$ 5 e 0,40% para saques, que já incluem a incidência tributária de PIS/Cofins e ISS.

Esses cenários servem de baliza para analisar os resultados, permitindo interpretar que, no caso da internalização das *exchanges*, o faturamento e a arrecadação estariam dentro do intervalo compreendido entre os cenários. Se espera que o efeito possa ser refletido em, no máximo, uma elevação dos valores até taxas atuais cobradas pelas nacionais e nacionalizadas (cenário B); e, no mínimo, que as taxas se mantenham as atuais (cenário A).

Em tese, com tais alterações nas taxas cobradas e na regulação⁹⁶, podem existir efeitos de migração de consumidores entre os dois tipos de *exchanges*. Por simplicidade, esses não são considerados nestes cenários.

Seguindo essa segmentação, os faturamentos foram estimados através da mesma metodologia utilizada no caso das *exchanges* nacionais e nacionalizadas, em que as taxas são aplicadas sobre o dimensionamento do mercado da seção 3. Ambos os cenários são apresentados no Gráfico 13.

Gráfico 13: Estimativa de faturamento das *exchanges* estrangeiras e parcialmente nacionalizadas nos cenários de internalização, em R\$ milhões (2021)



Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA Consultores.

⁹⁶ Teoricamente a sujeição das estrangeiras e parcialmente nacionalizadas atrai consumidores brasileiros para empresas deste tipo na medida em que as torna mais seguras. Por outro lado, se os custos adicionais regulatórios e tributários forem repassados aos consumidores por meio de taxas mais altas, espera-se que o aumento de preço (leia-se das taxas) resulte em uma menor contratação dos serviços destas. Nesse cenário de forças opostas operando sobre a dinâmica de migração de consumidores há muitas incertezas sobre a direção do vetor final, motivo pelo qual essa movimentação não foi incorporada na análise.

Ainda seguindo a metodologia aplicada no exercício realizado para as *exchanges* nacionais e nacionalizadas, incidiriam sobre o faturamento os tributos de prestação de serviços e de renda corporativa. Para estes as premissas e alíquotas utilizadas são análogas à seção anterior, ainda que a incidência de tais alíquotas seja diferente⁹⁷.

O principal ponto de distinção entre este exercício e o apresentado anteriormente é relativo ao cálculo do IOF, que requer uma premissa adicional, uma vez que o mercado de importações dimensionado pelo BCB é específico para empresas nacionais e nacionalizadas. Entende-se que existem, hoje, importações feitas por empresas estrangeiras ou parcialmente nacionalizadas, utilizando apenas criptoativos, de forma que não são realizados contratos cambiais. Com a internalização destas empresas supõe-se que esse processo, por requerer declarações à RFB, tenha que ser realizado por meios tradicionais, que envolveriam a necessidade de celebrar contratos de câmbio, forma de trocar os reais faturados no mercado interno para os dólares utilizados em suas sedes.

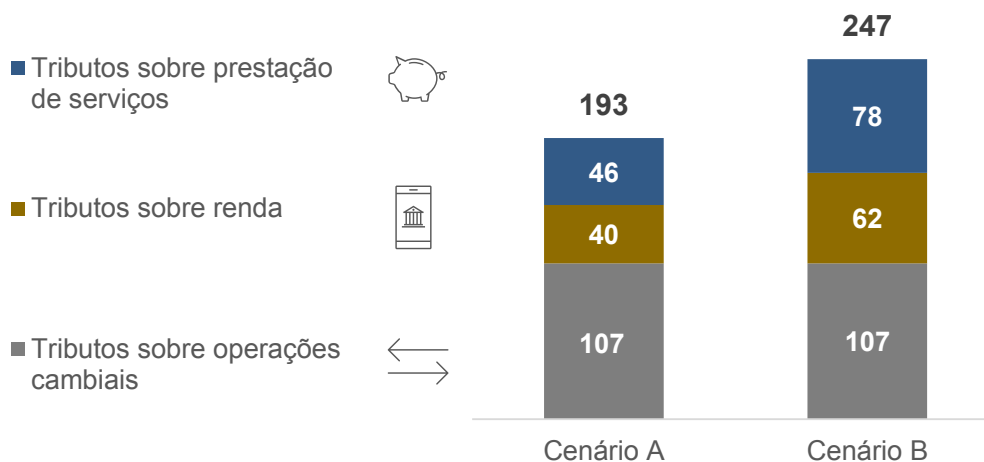
Com isso fez-se necessário dimensionar essa parcela de importações hoje “invisível”. A premissa utilizada foi de que o *share* mensal de importações de *exchanges* estrangeiras e parcialmente nacionalizadas é igual ao do mercado de transações. Desse modo, estima-se que em 2021 teria havido importação de R\$ 28,2 bilhões em criptoativos por essas *exchanges*, além dos R\$ 32,2 bilhões identificados pelo BCB.

Assim como no exercício apresentado acima, aplica-se a alíquota de IOF sobre o valor das importações, que por definição é o valor de operações cambiais realizadas. Estima-se então que se deixou de arrecadar aproximadamente R\$ 107 milhões em 2021 com a ausência de incidência de IOF sobre tais operações não reguladas. Observa-se que a arrecadação com esse tributo não difere entre os cenários uma vez que não depende das taxas cobradas pelas *exchanges*.

Dessa forma, como apresentado pelo Gráfico 14, se a tributação incidisse sobre as operações de *exchanges* com parte de sua operação situadas no exterior haveria potencial de aumento na arrecadação em até R\$ 247 milhões em 2021.

⁹⁷ As *exchanges* estrangeiras e parcialmente nacionalizadas, por não pagarem esses tributos, não terão em seus faturamentos (calculados utilizando as taxas atuais das estrangeiras e parcialmente nacionalizadas) o recolhimento tributário. Esse entendimento altera a forma como incidem os tributos, havendo necessidade de ajuste da base de incidência.

Gráfico 14: Estimativa de arrecadação nos cenários de internalização das exchanges estrangeiras e parcialmente nacionalizadas, em R\$ milhões (2021)



Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcoinity e BCB. Elaboração LCA Consultores.

Box 7: Cenário de importação de serviços das exchanges

Como alternativa à sujeição via internalização, as *exchanges* estrangeiras e parcialmente nacionalizadas poderiam passar a pagar tributos relativos à importação de serviços. É válido notar que essa alternativa atende apenas a solução de sujeição tributária, não garantindo que tais empresas estão operando em conformidade com outras práticas regulatórias, como por exemplo, o envio de informações para órgãos reguladores, hoje exigido pela IN 1.888/2019.

Premissas

Pressupõe-se que os serviços de tais *exchanges* passariam a ser tributados como serviços importados, com os tributos incidindo sobre faturamento líquido do cenário A, ou seja, as empresas manteriam as taxas cobradas atualmente. Optou-se por incidir os tributos sobre o faturamento com as taxas atuais uma vez que as taxas das *exchanges* nacionais e nacionalizadas já incluem os tributos pagos internamente.

Sobre esse valor calculado, chamado de valor do serviço, incidem geralmente seis tributos sobre serviços importados no Brasil, apresentados na

Tabela 7.

Tabela 7: Tributos sobre importação de serviços

Tributo	Base de cálculo	Alíquota
IRRF ¹	Valor do serviço ² + IRRF + CIDE + ISS	15% (geral, válida para serviços técnicos); 25% (não técnicos e "paraísos fiscais")

CIDE-Remessas	Idem a IRRF	10% (apenas para serviços técnicos)
ISS	Idem a IRRF	5% (a depender do município) ³
PIS/COFINS- Importação	Idem a IRRF + o próprio PIS/COFINS-Importação ⁴	9,25%
IOF	Valor do serviço acrescido da CIDE-Remessas	0,38%

*Notas: 1. Regime de incidência do IRRF pode provocar distorções competitivas uma vez que os serviços importados já são tributados em seu país de origem. Para evitar essa situação, é comum os parceiros celebrarem acordos bilaterais (ADTs). 2. Valor líquido dos tributos brasileiros recebido pelo prestador estrangeiro. 3. Premissa para esse exercício é de alíquota de 5% (cidade de São Paulo). 4. Segundo a IN RFB n. 1.911/2019, o PIS/COFINS-Importação para serviços deve ser calculado segundo a seguinte fórmula: $a * V * z$, onde: a é a alíquota; V é o valor da contratação, ou seja, valor recebido pelo prestador estrangeiro somado aos tributos retidos na fonte (IRRF, CIDE-Remessas e ISS); e $z = (1 + \text{alíquota do ISS}) / (1 - \text{alíquota do PIS/COFINS})$. Elaboração: LCA Consultores.*

Considera-se o serviço prestado pelas *exchanges* como técnico, com incidência de CIDE-Remessas. Premissa tem pouco impacto sobre os resultados, uma vez que serviços técnicos estão sujeitos a uma alíquota menor de IRRF na mesma proporção do CIDE-Remessas⁹⁸.

Entende-se também que não há aproveitamento de possíveis créditos do PIS-Cofins Importação, sendo tais serviços de intermediação em geral destinados ao consumidor final, geralmente uma pessoa física.

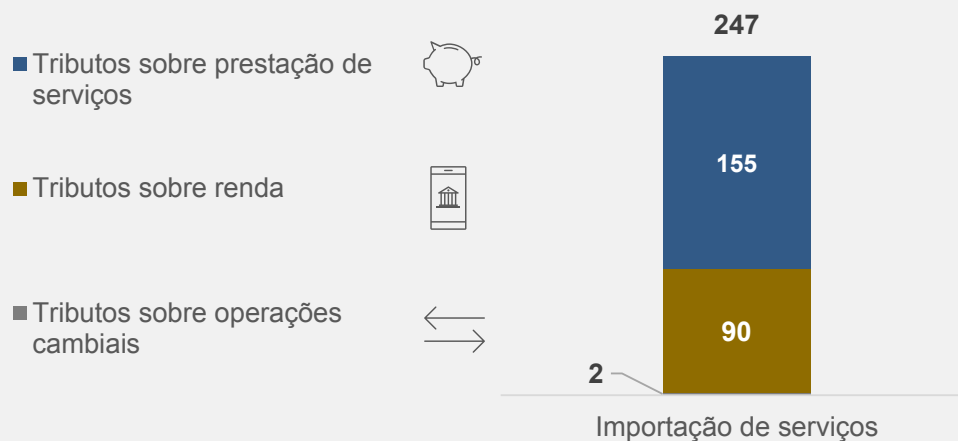
Resultados

O Gráfico 15 apresenta os resultados agregados por base de incidência, agregando PIS/Cofins-Importação, ISS e CIDE-Remessas como tributos sobre consumo, IRRF como tributo sobre renda e IOF como tributo sobre operações cambiais. Quando comparados aos dos cenários de internalização, destaca-se:

- Maior arrecadação com tributos sobre a prestação de serviços, devido à maior alíquota de PIS/Cofins e a incidência de CIDE-Remessas;
- Maior arrecadação de IR, pela alíquota de 15%, frente aos 10,88%, mesmo desconsiderando possível tributação de renda corporativa no país sede⁹⁹;
- Menor arrecadação de IOF pela diferença na base de incidência, agora relativa ao valor do serviço – nos cenários de internalização o tributo incidia sobre o valor total dos criptoativos nos contratos cambiais.

Gráfico 15: Estimativa de arrecadação nos cenários de importação de serviços das *exchanges* estrangeiras e parcialmente nacionalizadas, em R\$ milhões (2021)

⁹⁸ O único impacto dessa definição para o valor arrecadado é um aumento da base de cálculo do IOF, composta pela arrecadação do CIDE-Remessas. Entretanto, destaca-se que esse aumento tem poucos impactos sobre o valor final estimado.



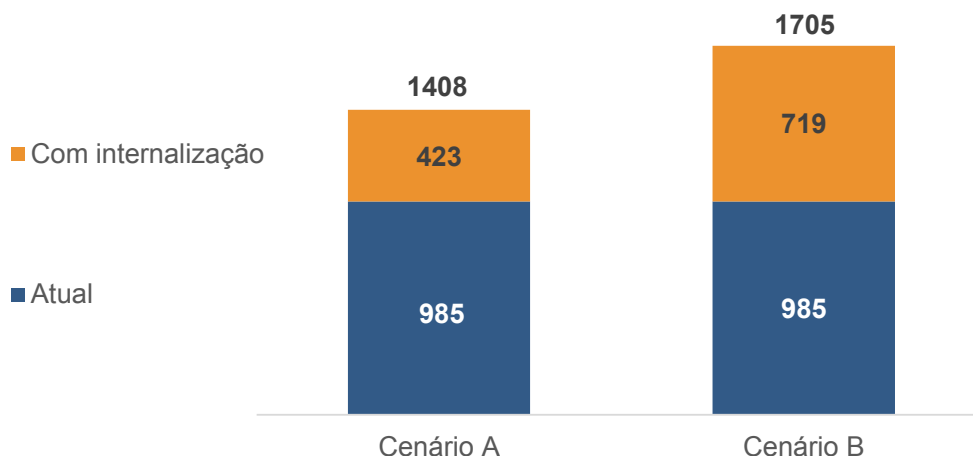
Nota: Considera-se o CIDE-Remessas como tributo sobre prestação de serviços. Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io, Bitcoinity e BCB. Elaboração LCA Consultores.

Dessa forma, é possível concluir que sujeição via importação de serviços aparenta ser uma alternativa desfavorável, de modo que provavelmente não seria escolhida pelas *exchanges* por implicar, em tese, em maior recolhimento tributário e conseqüentemente taxas mais altas ao consumidor. Observa-se que embora o valor arrecadado seja igual ao do cenário B de internalização, naquele o faturamento das empresas é significativamente superior, devido ao uso de taxas análogas às das empresas nacionais.

⁹⁹ Destaca-se que é possível que parte desses serviços já tenham sido tributados em seus países de origem. O Brasil possui alguns acordos que buscam evitar bitributação.

De forma resumida, os resultados indicam que o faturamento total agregado das *exchanges* ficaria entre R\$ 1,4 e R\$ 1,7 bilhões, conforme exposto no Gráfico 16.

Gráfico 16: Estimativa de faturamento total nos dois cenários apresentados, em R\$ milhões (2021)



Fontes: Diversas. Elaboração LCA Consultores.

Em termos de efeitos sobre a incidência tributária, conforme apresentado pela Tabela 8, as *exchanges* têm potencial de contribuir para o fisco com mais de meio bilhão de reais em ambos os cenários.

Tabela 8: Estimativa de arrecadação total nos dois cenários apresentados, em milhões (2021)

Cenário	Exchange	Prestação de serviços	Renda corporativa	Operações cambiais	Total
Cenário A	Atuais contribuintes	R\$ 85	R\$ 107	R\$ 122	R\$ 314
	Com internalização	R\$ 40	R\$ 46	R\$ 107	R\$ 193
	Total	R\$ 125	R\$ 153	R\$ 229	R\$ 507
Cenário B	Atuais contribuintes	R\$ 85	R\$ 107	R\$ 122	R\$ 314
	Com internalização	R\$ 62	R\$ 78	R\$ 107	R\$ 247
	Total	R\$ 147	R\$ 185	R\$ 229	R\$ 561

Fonte: CoinTrader Monitor, LiveCoins, CoinMetrics, Messari.io e Bitcoinity. Elaboração LCA Consultores

Conclusão

O presente estudo teve como objetivo apresentar um panorama geral da criptoeconomia, englobando discussões regulatórias e tributárias relativas a ela. Encontrou-se que os mercados da criptoeconomia estão em pleno desenvolvimento e manifestam características disruptivas que trazem novidades e incertezas. Esse cenário apresenta significativas implicações regulatórias e tributárias, dificultando a construção de diretrizes amplas e sistemáticas para o setor, de modo que não há consenso sobre quais seriam as boas práticas regulatórias que deveriam ser estabelecidas para garantir maior eficiência aos mercados.

Frente a esses desafios, cooperação internacional e análise comparativa de legislações contribuem para a construção do arcabouço legal para operações de criptoativos no Brasil, que atualmente possui normas para o setor que podem falhar em abrangência e objetividade. O PL 4.401/2019, em discussão no Congresso Nacional, se apresenta como principal caminho para a criação de um marco regulatório para as atividades do setor.

Ainda quanto ao funcionamento do mercado, destaca-se o aumento significativo observado no valor dos ativos, além de um processo de diversificação de tipos e funções dos ativos existentes. De maneira concomitante esses fenômenos têm impulsionado o crescimento da criptoeconomia. Estima-se que, no Brasil, em 2021, foram transacionados R\$ 317 bilhões em criptoativos pelas *exchanges*, o que representou um aumento de 513,6% com relação ao mesmo valor em 2020, para além disso, destaca-se como informações importantes encontradas:

- Em maio de 2022, 620.915 CPFs distintos transacionaram criptoativos, valor máximo da série computada pela RFB;
- É crescente o número de investidores institucionais, sendo o valor máximo encontrado de 8.591 CNPJ distintos que transacionaram criptoativos em um mesmo mês;
- Desde janeiro de 2019, foram identificados cerca de 10 mil empregos gerados pela CNAE que engloba agentes da criptoeconomia;
- A proporção média de bitcoins no total transacionado de criptoativos é de aproximadamente 33%;

- O BCB estimou a importação do equivalente a US\$ 6 bilhões, ou R\$ 32,2 bilhões¹⁰⁰, em 2021;
- Foram identificadas 35 empresas transacionando criptoativos no Brasil em 2021, e embora apenas 7 delas não tenham domicílio no Brasil, 42% do valor foi transacionado nestas *exchanges*, no mesmo ano.

O atual mercado de intermediação de criptoativos é caracterizado pela presença de diferentes modelos de negócios de *exchanges* no Brasil. Estas se diferenciam, entre diversos outros aspectos, pela possibilidade de *enforcement* de normas regulatórias e pela sujeição à incidência de tributos nacionais sobre a intermediação de criptoativos. Essa diferença leva a ausência de recolhimento de tributos sobre operações de intermediação de criptoativos por parte das *exchanges* estrangeiras e parcialmente nacionalizadas.

Estima-se que, em 2021, as *exchanges* teriam capacidade de contribuir com cerca de R\$ 314 bilhões para o fisco, devido ao pagamento de tributos sobre prestação de serviços, renda e operações cambiais. Caso fossem sujeitas aos mesmos tributos, as *exchanges* estrangeiras e parcialmente nacionalizadas contribuiriam, em uma estimativa conservadora, com R\$ 193 milhões.

¹⁰⁰ Taxa de câmbio comercial de compra média mensal (BCB).

Anexos

Anexo 1: Divisão das exchanges e cálculo de taxas

A Tabela 9 apresenta informações detalhadas das exchanges de criptoativos que operaram no Brasil em 2021.

Tabela 9: Exchanges utilizadas na análise, taxas de maio de 2022

Exchange	Classificação	Share 2021	Share 2020	Taxa de ordem	Fixo Saque	Variável Saque	CNAE 6619-3/99
Binance	Estrangeira	29,8%	1,3%	0,10%	R\$ 2,60	0,00%	Não registrada
BitPreço	Nacional	13,4%	12,0%	0,20%	R\$ 4,90	0,20%	Atividade secundária
MercadoBitcoin	Nacional	13,2%	21,5%	0,70%	R\$ -	0,00%	Atividade secundária
NovaDAX	Nacionalizada	12,3%	15,1%	0,50%	R\$ 8,90	1,50%	Atividade principal
BitcoinToYou	Parcialmente Nacionalizada	8,7%	10,2%	0,60%	R\$ 9,99	1,89%	Não registrada
Foxbit	Nacional	3,8%	5,8%	0,50%	R\$ -	0,00%	Não registrada
FTX	Estrangeira	2,8%	0,6%	0,07%	R\$ 10,00	0,30%	Não registrada
Coinext	Nacional	2,5%	4,3%	0,50%	R\$ 8,99	0,19%	Atividade principal
BitcoinTrade	Nacionalizada	2,4%	6,4%	0,50%	R\$ 4,90	0,00%	Atividade principal
PagCripto OTC	Nacional	2,3%	0,7%	0,25%	R\$ 10,00	0,00%	Atividade principal
UpCâmbio	Nacional	1,5%	0,9%	0,25%	R\$ 10,00	0,35%	Não registrada
YouBtrade	Nacional	1,1%	0,6%	0,30%	R\$ 9,90	0,00%	Atividade principal
Bisoint	Nacional	0,9%	0,9%	0,00%	R\$ 14,90	0,00%	Atividade secundária
Brasil Bitcoin	Nacional	0,8%	1,7%	0,50%	R\$ 5,00	0,50%	Não registrada
Makes Exchange	Nacional	0,7%	1,5%	0,00%	R\$ -	0,00%	Atividade secundária
Demais Nacionais	Nacional	3,0%	16,4%	-	-	-	-
Demais Parc. Nacionalizadas	Parcialmente Nacionalizada	0,8%	0,1%	-	-	-	-

Nota: Cálculo das taxas médias de nacionais e estrangeiras foi realizado através de uma média ponderada pelo share das exchanges, em que foram consideradas todas as empresas com dados disponíveis na data de coleta. A tabela apresenta apenas as exchanges com share maior que 0,5%, o restante das empresas foi agregada nas linhas "Outras".

Classificação: Existem empresas estrangeiras com CNPJ no Brasil e quadro societário composto apenas por pessoas jurídicas situadas no exterior, no entanto elas foram classificadas dessa forma por possuir empresa filiada no exterior (exemplo: BitcoinToYou e BitcoinToYou Internacional). As empresas nacionalizadas foram definidas por participarem de Holdings no exterior (NovaDAX – China e BitcoinTrade/Ripio – Ilhas Cayman).

Fonte: CoinTrade Monitor, em maio de 2022. Elaboração LCA Consultores.

Anexo 2: Pedidos de dados via Lei de Acesso à Informação (LAI)

1. Tema: Custódia de Criptoativos. Órgão: BCB.

Demanda: Solicito melhor entendimento sobre quais tipos de informação o Banco Central possui sobre a custódia de criptoativos. Informações como está enunciada pelo presidente do BC, citada abaixo, derivam de contratos de câmbio, importação de criptoativos, *market-makers*, ou de informações da Receita Federal? Quais bases de dados o BC dispõe sobre o assunto? Estas são públicas? "O presidente do BC destacou ainda que os criptoativos cresceram mais no Brasil como investimento do que como meio de pagamento e destacou que há concentração de custódia desses ativos. "83% dos ativos em cripto estão em quatro custodiantes", afirmou."

Data de Resposta: 25/06/2022.

Resposta: O Banco Central não possui informação oficial sobre custódia de criptoativos. O dado mencionado pelo presidente provém de informação preliminar sobre o assunto.

2. Tema: Importação e Exportação de Criptoativos. Órgão: BCB.

Demanda: Solicito, por gentileza, as séries mensais completas de importação e exportação de criptoativos, em todos os anos em que estas estiverem disponíveis. Também solicito informações adicionais de como é feita a estimativa destes. Os contratos de câmbio de criptoativos são estimados através de informações de *exchanges*?

Data de Resposta: 02/06/2022.

Resposta: A fonte das exportações e das importações de criptoativos é o contrato de câmbio, que pode ser realizado por qualquer residente (pessoa física ou pessoa jurídica, *exchange* ou não). Entretanto, operadores de grande porte têm predominado como contraparte residente desses contratos de câmbio. A identificação da operação vinculada ao criptoativo é realizada por meio de um código cambial e um campo texto em que a parte residente do contrato de câmbio presta essa informação. Cabe lembrar que, por definição, importação e exportação referem-se à mudança de propriedade (no caso do criptoativo) entre residente e não residente. Portanto, compras/vendas de

criptoativos entre residentes, diretamente no mercado doméstico, não fazem parte do escopo dessas séries.

3. Tema: Criptoativos – PJ por CNAE. Órgão: RFB.

Demanda: Solicito as informações de valor declarado em criptoativos por PJs, segregado por uso de *exchanges* no exterior e sem uso de *exchanges*, no maior nível de desagregação por CNAE possível. Solicito esta informação para todos os meses em que esta estiver disponível.

Data de Resposta: 22/07/2022.

Resposta: Em atenção à sua solicitação, informamos que dados abertos sobre as operações de criptoativos estão disponíveis no site da Receita Federal do Brasil. Solicitações contempladas pelos dados já publicados deixam de ser atendidas com base no inc. II do art. 13 do Decreto nº 7.724, de 2012.

4. Tema: Criptoativos – Exchanges nacionais e exchanges no exterior. Órgão: RFB.

Demanda: Solicito o modo no qual a Receita Federal do Brasil diferencia *exchanges* nacionais e *exchanges* no exterior, e se esta classificação sofreu alguma alteração desde que os dados de declarações em criptoativos passaram a ser obtidos.

Data de Resposta: 22/07/2022.

Resposta: Em atenção à sua solicitação, informamos que a classificação é feita com base no domicílio tributário da *exchange*. Não houve mudança nessa orientação. As domiciliadas no país estão obrigadas a prestar informações à Receita Federal. No caso de operações realizadas fora de *exchange* ou em *exchange* no exterior, as informações devem ser prestadas pela pessoa que realizar a operação com criptoativo.

5. Tema: Criptoativos - Pessoas Físicas Declarantes. Órgão: RFB.

Demanda: Solicito informações sobre o perfil das pessoas físicas declarantes de criptoativos no menor nível de agregação possível. O relatório nº 3 dos dados abertos da RFB apresenta o nº de operações e valor de operação por sexo: solicito estas informações também estratificadas por idade, nível de renda, ocupação dos indivíduos e unidade federativa de domicílio. Solicito esta informação para todos os anos em que ela estiver disponível.

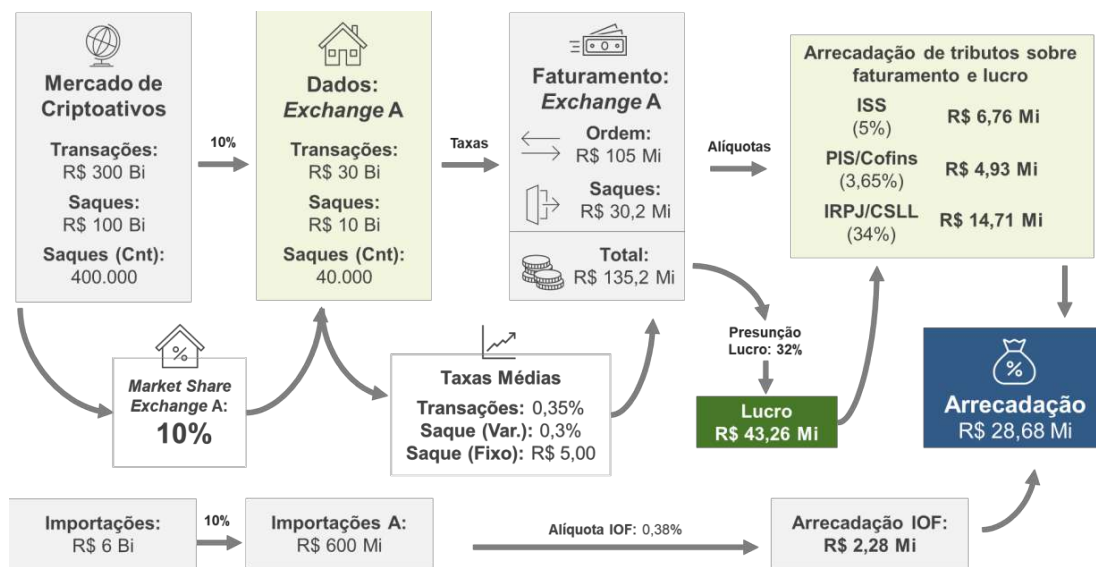
Data de Resposta: 19/08/2022.

Resposta: Em atenção à sua solicitação, informamos que os dados estão disponíveis apenas no nível de agregação divulgado no relatório 3 citado pelo solicitante. O fornecimento da informação na forma solicitada envolve trabalhos adicionais de análise, interpretação ou consolidação de dados.

Anexo 3: Exemplificação da metodologia – exchange fictícia

A Figura 8 apresenta a metodologia utilizada na estimativa de arrecadação tributária aplicada a uma *exchange* fictícia, visando facilitar o entendimento através dos cálculos realizados no exercício hipotético.

Figura 8: Exemplificação da metodologia através de exchange fictícia



Anexo 4: Comparação dados agregadores e RFB

Exceto o dado relativo de importações e exportações, a maior parte dos outros dados apresentados neste parecer provêm de dois tipos de fonte:

1. Parte significativa dos dados é fornecida pela Receita Federal Brasileira. O órgão congrega informações declaradas por pessoas físicas e jurídicas, em conformidade com a IN 1.888/2019, mesmo quando as operações são feitas fora do livro aberto¹⁰¹. A RFB possui critério próprio para segmentar as *exchanges* entre nacionais e estrangeiras, informando via Lei de Acesso à Informação (LAI)¹⁰² que segmenta as *exchanges* de acordo com domicílio fiscal¹⁰³.
2. Tais dados serão complementados por informações obtidas via agregadores, que são sites que computam todas as operações feitas em livro aberto, embora não observem transações realizadas por OTCs. Foram utilizados dados do *CoinTrader Monitor* e do *LiveCoins*¹⁰⁴, para valores transacionados em *exchanges*¹⁰⁵. Para além destes utilizou-se o *Messari.io*, o *Bitcoinity* e o *Coinmetrics* para as informações necessárias na metodologia de estimativa de saques, além do *Coin Marketcap*, referência para os dados gerais do mercado, apresentados na seção 2. Os dados dessas fontes foram segmentados de acordo com a classificação apresentada na seção 3. Para fins de comparação com a base da RFB considera-se como nacionais também as nacionalizadas e como estrangeiras também as parcialmente nacionalizadas.

Devido à obrigatoriedade imposta pela IN 1.888 em reportar transações, dados para *exchanges* nacionais são coerentes entre a RFB e os agregadores. Entretanto, a RFB observa apenas parte diminuta das transações feitas em estrangeiras, como apresentado no Gráfico 17, uma vez que elas não precisam se conformar a IN por não possuírem domicílio no país. Para esse grupo de *exchanges* as informações foram prestadas pela pessoa física que realizou a operação com criptoativos.

Gráfico 17: Evolução do mercado de transações de criptoativos em *exchanges* nacionais e estrangeiras, por base de dados

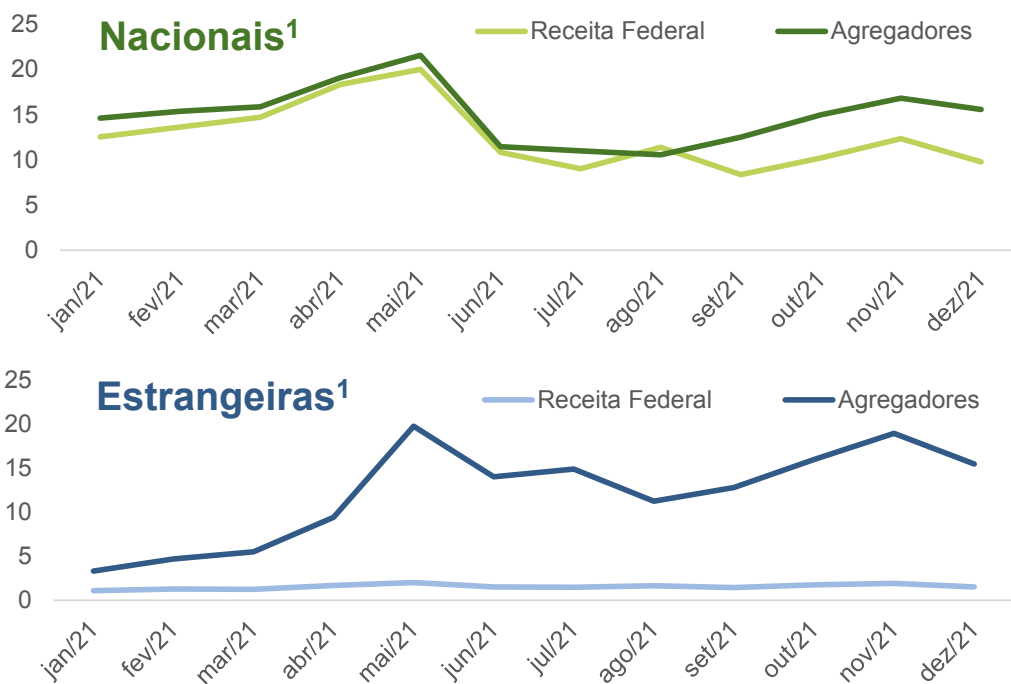
¹⁰¹ Realizadas em OTCs e parte das operações P2P, que representam aproximadamente 16% do total declarado.

¹⁰² O Anexo 2 resume os pedidos de informação via LAI feitos.

¹⁰³ A RFB declarou: “*informamos que a classificação é feita com base no domicílio tributário da exchange*”.

¹⁰⁴ Para além destes utilizou-se o *Messari.io*, o *Bitcoinity* e o *Coinmetrics*.

¹⁰⁵ Segundo a fonte: “*Esses dados são coletados diretamente das API disponibilizadas pelas próprias exchanges. Considera-se que as informações oferecidas através destes canais são DECLARAÇÕES e que não foram submetidas a auditoria externa*”.



Nota: 1. Para essa comparação considerou-se como nacionais também as nacionalizadas, e como estrangeiras também as parcialmente nacionalizadas. 2. Informações do CoinTradeMonitor são originalmente restritas ao BTC, entretanto o mercado é corrigido com através da informação de proporção do BTC no mercado nacional, disponibilizado pelo LiveCoins. Fontes: CoinTrade Monitor, Livecoins e Receita Federal do Brasil. Elaboração LCA Consultores.

Essa comparação de informações endossa a classificação realizada neste trabalho e indica que os dados dos agregadores possuem maior abrangência ao visualizar as transações feitas por brasileiros através de *exchanges* estrangeiras, motivo pelo qual este trabalho optou por utilizá-los no dimensionamento apresentado.

Ficha técnica

Panorama setorial da criptoeconomia no Brasil

Equipe técnica

Gustavo Madi Rezende – Diretor de Economia do Direito, Mestre em Economia.

Verônica Lazarini Cardoso – Gerente de Projetos, Mestre em Economia.

Pedro Salerno – Analista de Projetos, Mestre em Economia.

Bernardo Riatto Perrotti – Analista de Projetos, Graduando em Economia.

João Pedro de Paula e Silva – Estagiário, Graduando em Economia.

LCA Consultores

Rua Cardeal Arcoverde, 2450, Conjunto 301 - São Paulo, SP

Fone: 11 3879-3700 | Fax: 3879-3737

Site: www.lcaconsultores.com.br