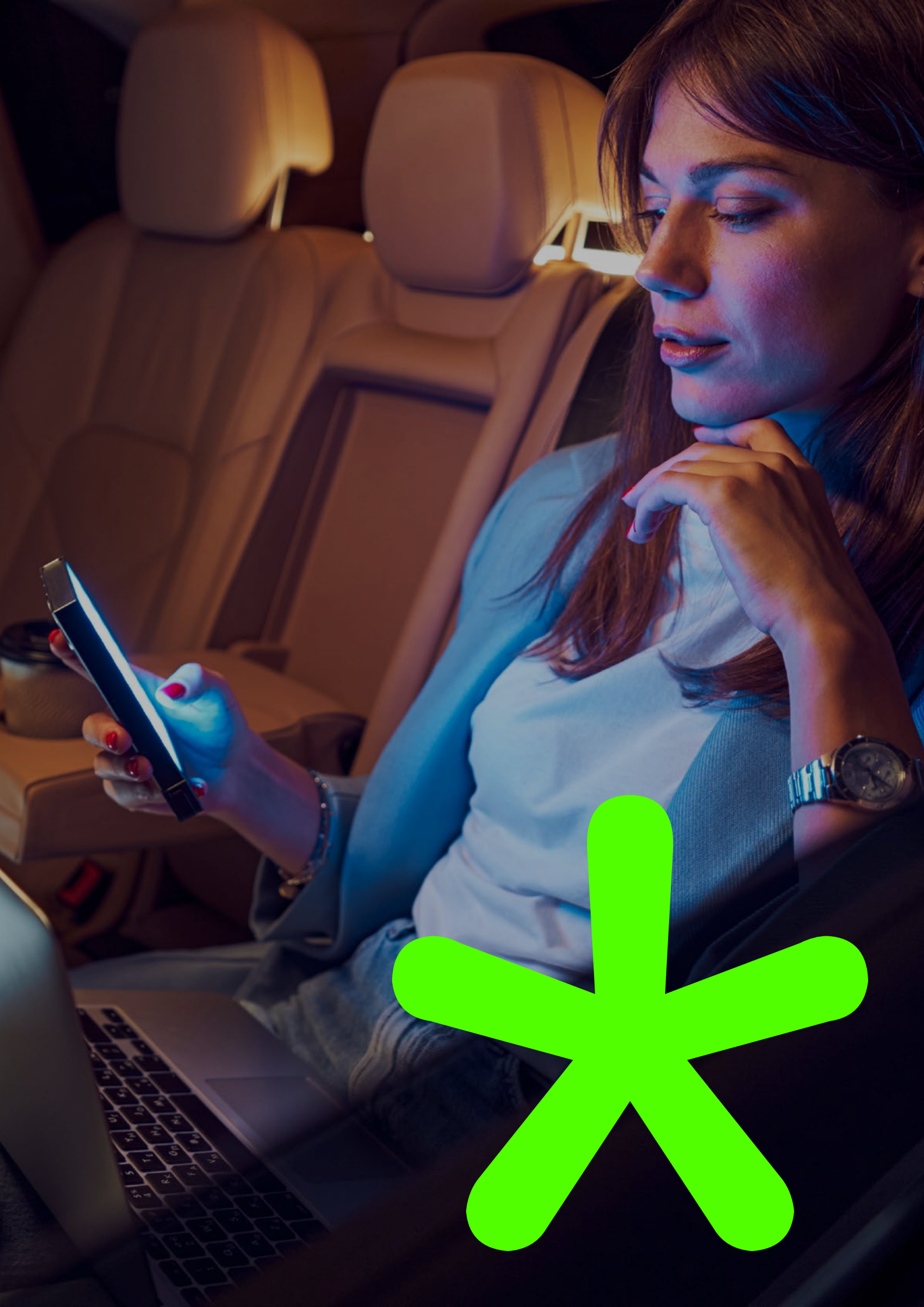
glossário abcripto*

2023

CVM
Comissão de Valores Mobiliários



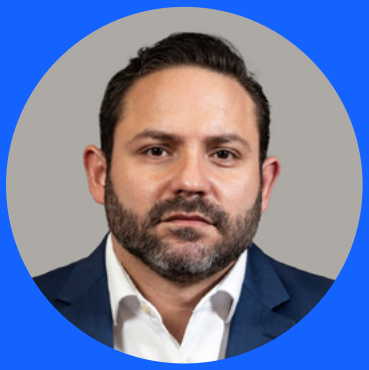
.intro

Este documento provê uma proposta para um glossário de termos relativos à área de criptomoedas, ativos digitais, tokenização e áreas correlatas que visando atingir os seguintes objetivos:

- **Padronizar a terminologia;**
- **Facilitar o diálogo entre os membros da ABCRIPTO em si e a sociedade em geral;**

Espera-se que esse documento seja ampliado e revisado periodicamente para incorporar as sugestões recebidas e dar conta das novidades surgindo na área.

Favor enviar sugestões, correções, críticas, opiniões para: **pesquisaeducacao@abcripto.com.br**

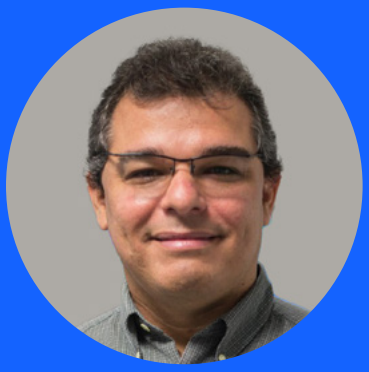


Bernardo Srur
Diretor Presidente da ABcripto

A Associação Brasileira de Cripteconomia - ABcripto, em parceria com a Comissão de Valores Mobiliários (CVM), tem a satisfação de apresentar à sociedade brasileira o primeiro Glossário com expressões técnicas esclarecidas sobre finanças descentralizadas (DeFi) e outras aplicações relativas à criptoeconomia, blockchain e investimentos em ativos digitais. O glossário é um orgulho para a ABcripto e para a CVM. É uma obra com rigor técnico, qualidade editorial, produzida a várias mãos.
O material oferece conhecimento e estrutura para o desenvolvimento e a inserção de todos no mercado de ativos digitais

Fábio Moraes
Coordenador do Comitê de Pesquisa e Educação da ABcripto

O Glossário sobre criptoeconomia feito pela ABcripto representa uma importante contribuição para ampliar o mercado, atrair investidores e democratizar o acesso aos produtos financeiros cripto, que vieram para aumentar a inclusão financeira e a desintermediação das relações entre o setor financeiro e a sociedade. O Glossário é uma obra viva e sempre refletirá as mudanças e evolução do mundo cripto.



Marco Carnut
Vice Coordenador do Comitê de Pesquisa e Educação da ABcripto

O Glossário contém, até o momento, verbetes listados em ordem alfabética - o qual possuem uma ou mais acepções, que são descrições sucintas do seu significado. O dicionário tem como objetivo justamente facilitar a compreensão de expressões ligadas ao mercado de ativos digitais e estreitar o diálogo entre os membros da ABcripto, da CVM e a sociedade em geral

metodologia

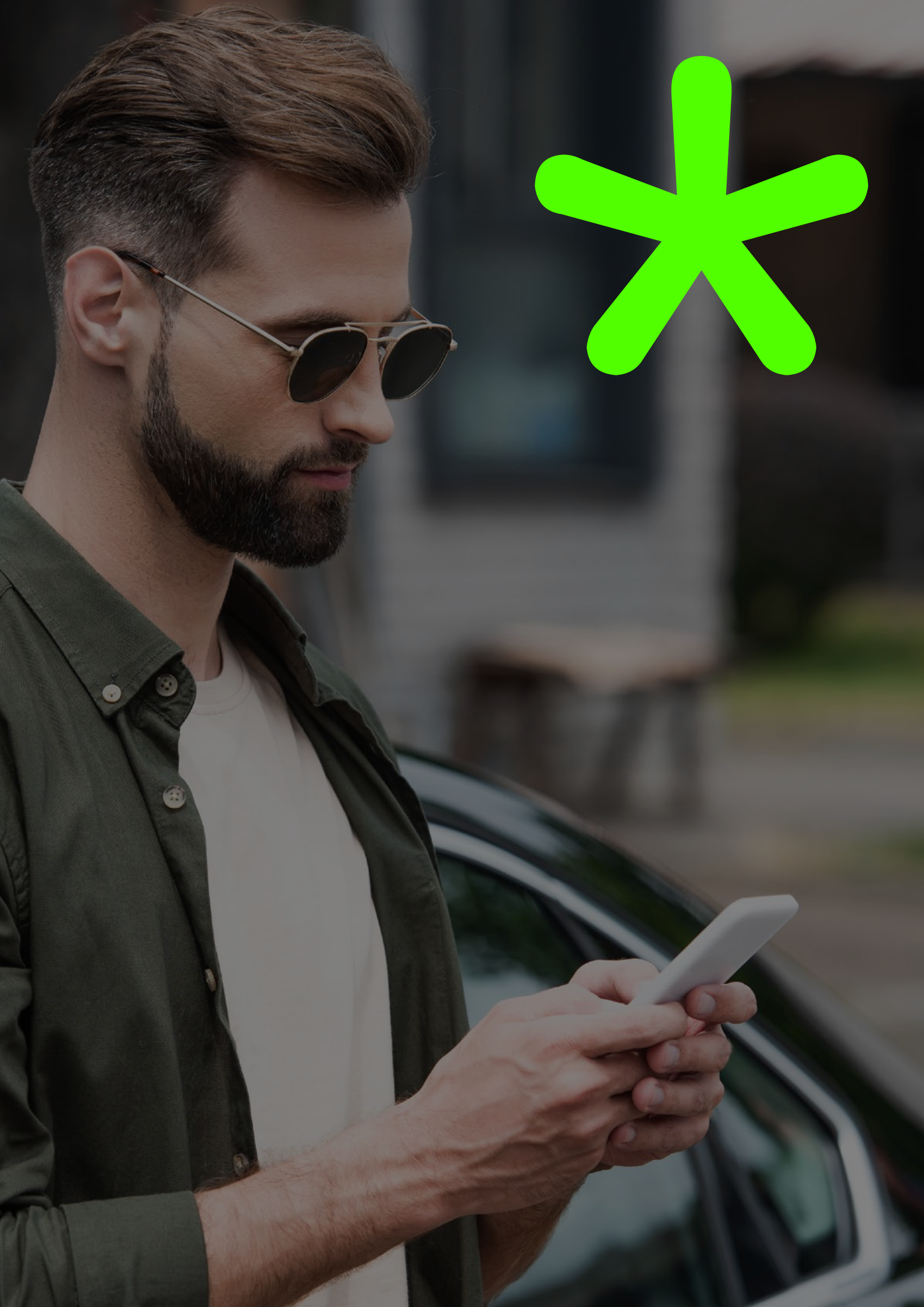
Os participantes do GT acrescentaram verbetes para consideração, juntamente com uma proposta de definição, que foram revistas e aprimoradas em sucessivas reuniões.

Tentou-se almejar:

- **Brevidade:** as acepções devem ser as mais sucintas possíveis. Exceto em conceitos especialmente complexos ou com muitas acepções, deveria ser possível manter os verbetes com quatro linhas ou menos;
- **Clareza:** as acepções devem ser compreensíveis pelo público mais amplo possível;
- **Rigor:** deve ser possível atingir um amplo consenso de que as acepções estão "corretas", ou seja, não ferem conceitos e princípios das áreas de conhecimento de onde se originam;
- **Aderência à legislação:** certas leis já definem certos conceitos e os verbetes devem se ater às definições legais;
- **Utilidade:** as definições devem ajudar a avançar os propósitos e interesses da associação, facilitando a comunicação entre seus membros e a sociedade em geral.

Tenta-se evitar:

- **Contradições:** verbetes ou acepções que conflitem logicamente entre si.



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 minuciosa 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 Laudering", 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

❶ sigla de "All Time High", *veja*: ☛ alta histórica;

ativo

❶ 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

❶ 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

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

atomic swap

❶ mesmo que: ☛ troca atômica.

atômico

❶ 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

❶ 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 "bc1" e os da testnet com "tb1".*

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".*

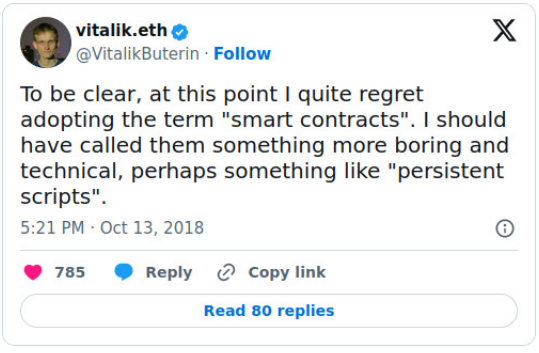
- *A perspectiva ampla sobre contratos inteligentes é que, mesmo sendo apenas programas de computador, eles executam vontades pré-acordadas entre partes, daí o termo "contrato".*

- *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

❶ 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

❶ (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 implementaçao 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

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

ETH

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

ether

❶ (tipicamente pronunciado pelos brasileiros como "éter", soa mais como "íter" quando falado pelos estrangeiros; símbolo: Ξ) unidade de conta da criptomoeda Ethereum. ❷ 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

❶ (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; ❷ 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

❶ (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

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

EVM

❶ abreviatura de "Ethereum Virtual Machine", *veja* ☛ ethereum virtual machine; ❷

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 Efígie 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, "colecionáveis" – 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 gigawei.*

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

ℹ 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

ℹ 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, quantos identificadores de transações e blocos são tradicionalmente grafados em hexadecimal.*

hodl

ℹ (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

ℹ 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

❶ *mesmo que*: ☛ armazenamento quente;

hot wallet

❶ *mesmo que*: ☛ armazenamento quente;

kibi-

❶ (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-

❶ (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

❶ abreviatura de "Initial Coin Offering", *vide* ☛ initial coin offering.

initial coin offering

❶ 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

❶ 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

❶ *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: Ł) 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 costumer", 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

❶ (gíria) indivíduo propenso a vender seus ativos em pânico, sob preços ou condições desfavoráveis, perdendo dinheiro ou oportunidades. *Veja também:* ☛ alfaçar.

market cap

❶ *contração de "market capitalization":* ☛ capitalização de mercado.

market capitalization

❶ *mesmo que:* ☛ capitalização de mercado.

maxi

❶ *contração de:* ☛ maximalista.

📖 *"Depois de se queimar tanto com as alts, ele acabou se tornando maxi."*

📖 *"Aquela conferência só dá maxi."*

maximalista

❶ 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-

❶ (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

❶ 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 descrevedo 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

ℹ 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

ℹ 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

ℹ ("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-

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

📖 *Um gigawei (Gwei) é um nanoether.*

não-permissionado

ℹ 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 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

❶ (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

❶ (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

❶ (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

❶ 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

❶ 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

❶ 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. ❷ 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

❶ 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

❶ *mesmo que*: ☛ testemunhas segregadas.

segwit

❶ abreviatura de "segregated witness", *veja:* ☛ testemunhas segregadas.

semente

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

privadas, e, por conseguinte, endereços de recebimento. ❷ 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

❶ (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

❶ (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 dígitios decimais). *Veja também:* ☛ hash..

shill

❶ 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

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

simplified payment verification

❶ *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-

❶ (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

❶ ("*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-

❶ (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

❶ ("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

❶ *mesmo que:* ☛ token de utilidade.

valor mobiliário

❶ 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

❶ (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

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

web1

❶ 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

❶ 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

❶ 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

❶ 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 Olimpia, SP, 04552-020
São Paulo - SP

contato@abcripto.com.br

CVM
Comissão de Valores Mobiliários

abcripto.com.br

linkedin.com/abcripto

@ABCriptoOficial

@abcripto