GLOSSÁRIO COMPLETO CRIPTO & INVESTIGAÇÃO

Investigate X – Termos essenciais, riscos, segurança, operacional e jurídico para profissionais e iniciantes

1. ESSENCIAL (A–Z)

Address (Endereço)

Código público único associado a uma carteira em uma blockchain, usado como ponto de destino ou origem para transferências.

Exemplo: Sempre verifique o endereço antes de enviar qualquer valor, mesmo que seja uma pequena quantia de teste.

Airdrop

Distribuição gratuita de tokens para endereços selecionados, geralmente para promover um projeto ou recompensar usuários ativos.

Exemplo: Projeto novo faz airdrop de 100 tokens para quem tiver mais de 1 ETH na carteira ao final da semana.

Altcoin

Qualquer criptomoeda que não seja Bitcoin, incluindo Ethereum, Solana, Cardano e milhares de outras.

Exemplo: Mercado de altcoins costuma subir forte quando o Bitcoin entra em consolidação.

Asset (Ativo)

Bem digital com valor econômico negociável, como uma moeda, token, NFT ou direito representado na blockchain.

Exemplo: NFTs de arte digital se tornaram ativos colecionáveis com valores na casa de milhões de dólares.

Autocustódia

Modelo em que o usuário mantém controle total sobre suas chaves privadas, assumindo responsabilidade por segurança e recuperação.

Exemplo: Com autocustódia, o usuário é seu próprio banco, sem depender de terceiros.

Balance (Saldo)

Quantidade de ativos disponíveis para uso em uma carteira ou endereço específico.

Exemplo: Verifique o saldo do endereço receptor antes de confirmar uma transferência grande.

Bitcoin (BTC)

Primeira e maior criptomoeda por capitalização, criada em 2009, vista como reserva de valor e 'ouro digital'.

Exemplo: Investidores institucionais alocam parte do portfólio em Bitcoin como proteção contra inflação.

Blockchain

Registro compartilhado em que as informações são organizadas em blocos ligados uns aos outros, de forma que, depois de confirmadas, se tornam extremamente difíceis de alterar.

Exemplo: Quando um golpe acontece, o caminho do dinheiro pode ser acompanhado porque a blockchain guarda todo o histórico.

Bridge (Ponte)

Protocolo que permite mover ativos de uma blockchain para outra, criando versões equivalentes em diferentes redes.

Exemplo: Usuários movem USDC de Ethereum para Solana via bridge para aproveitar taxas menores.

CEX (Exchange Centralizada)

Plataforma de negociação controlada por empresa, que gerencia custódia, ordens e conformidade regulatória.

Exemplo: Corretoras CEX são obrigadas por lei a congelar endereços ligados a sanções internacionais.

Carteira (Wallet)

Ferramenta que armazena e gerencia chaves criptográficas, permitindo ao usuário consultar saldos, assinar transações e interagir com aplicações da rede.

Exemplo: Você pode ter uma carteira instalada no computador apenas para análise e outra, em hardware, reservada para guardar valores maiores.

Chave Privada (Private Key)

Informação sigilosa que permite autorizar transações a partir de uma carteira; em termos práticos, quem domina essa chave controla os fundos associados.

Exemplo: Se um golpista obtiver a chave privada, ele consegue mover todos os ativos daquele endereço sem pedir mais nenhuma confirmação.

Confirmações

Quantidade de blocos que foram adicionados à cadeia depois da inclusão de uma transação específica, aumentando a dificuldade de revertê-la.

Exemplo: Algumas corretoras só liberam saques após um número mínimo de confirmações, como medida adicional de segurança.

Criptoativo / Ativo Virtual

Representação de valor que existe apenas de forma digital e usa técnicas de criptografia para controlar emissão, transferência e autenticação das operações na rede.

Exemplo: Uma pessoa pode receber pagamento por um serviço em ativos virtuais, sem passar por banco tradicional.

Custódia

Modelo em que uma empresa mantém as chaves privadas dos clientes e assume responsabilidade pela segurança e recuperação dos ativos.

Exemplo: A maioria dos brasileiros usa custódia em corretoras para facilitar o dia a dia.

DeFi (Finanças Descentralizadas)

Ecossistema de serviços financeiros (empréstimos, trocas, derivativos) que rodam em contratos inteligentes, sem bancos tradicionais.

Exemplo: Protocolos DeFi permitem que qualquer pessoa empreste cripto e receba juros automaticamente.

Endereço (Wallet Address)

Código público associado a uma carteira em determinada rede, usado como destino ou origem de envios, de forma semelhante a um número de conta.

Exemplo: Antes de autorizar o envio, compare o endereço caracter por caracter para evitar transferir fundos para o endereço errado.

Fiat

Moeda emitida por governo central (Real, dólar, euro), usada como entrada e saída do ecossistema cripto.

Exemplo: PIX é o principal método de entrada fiat para comprar cripto no Brasil.

Gas / Taxa de Rede

Valor pago para que uma operação seja processada e incluída na blockchain, remunerando os participantes que validam e registram as transações.

Exemplo: Em momentos de rede congestionada, usuários aceitam pagar taxas mais altas para que suas transações sejam confirmadas mais rapidamente.

Hash

Resultado matemático único de uma função criptográfica, usado para identificar blocos, transações e garantir integridade dos dados.

Exemplo: O hash de um bloco contém o hash do bloco anterior, formando a cadeia que dá segurança à blockchain.

1. ESSENCIAL (A–Z) — continuação

Layer 1 (L1)

Blockchain principal que provê consenso, segurança e processamento nativo (Bitcoin, Ethereum, Solana).

Exemplo: Ethereum é uma Layer 1 que suporta milhares de contratos inteligentes simultâneos.

Layer 2 (L2)

Soluções construídas sobre uma L1 para melhorar velocidade e reduzir custos, mantendo a segurança da rede base.

Exemplo: Rollups como Arbitrum processam centenas de transações por segundo com taxas muito menores que a Ethereum principal.

NFT (Non-Fungible Token)

Token único que representa propriedade sobre um item digital ou físico específico, não intercambiável com outros.

Exemplo: Uma obra de arte digital vendida como NFT pode ser revendida várias vezes na blockchain.

Node (Nó)

Computador que participa da rede, armazenando cópias da blockchain e validando novas transações e blocos.

Exemplo: Nós completos armazenam toda a blockchain desde o primeiro bloco (genesis block).

Off-ramp

Serviço que converte criptoativos em moeda fiduciária tradicional, permitindo saques para contas bancárias.

Exemplo: Vender cripto na corretora e transferir via TED é um exemplo clássico de off-ramp.

On-ramp

Serviço que permite converter moeda fiduciária em criptoativos, sendo a porta de entrada para novos usuários.

Exemplo: Comprar Bitcoin via PIX em uma corretora brasileira é um on-ramp muito usado.

P2P (Peer-to-Peer)

Transação direta entre duas pessoas, sem intermediários como bancos ou corretoras.

Exemplo: Plataformas P2P conectam quem quer vender cripto diretamente com quem quer comprar, sem custódia central.

Public Key (Chave Pública)

Informação derivada da chave privada que serve para gerar endereços e verificar a autenticidade de transações assinadas.

Exemplo: A partir da chave pública, qualquer pessoa pode gerar o endereço para enviar fundos.

1. ESSENCIAL (A–Z) — continuação

Rede EVM

Conjunto de redes compatíveis com a máquina virtual da Ethereum, o que permite que o mesmo tipo de contrato e carteira funcione em diferentes blockchains.

Exemplo: Uma carteira configurada para Ethereum pode ser facilmente ajustada para interagir com outras redes EVM, como BNB Chain ou Polygon.

Seed Phrase (Frase-Semente)

Lista de palavras gerada pela carteira que serve como mecanismo de restauração: a partir dela, é possível recriar as chaves e recuperar o acesso aos fundos.

Exemplo: Em caso de perda ou quebra do dispositivo, basta reinstalar a carteira e inserir a frase-semente anotada em papel para resgatar os endereços.

Smart Contract (Contrato Inteligente)

Programa que roda na blockchain e executa automaticamente condições pré-definidas, sem necessidade de um operador humano intermediando cada passo.

Exemplo: Pools de liquidez, bridges e muitas DEX funcionam quase inteiramente por meio de contratos inteligentes.

Token (ERC-20) e NFT

Tokens fungíveis seguem padrões técnicos (como ERC-20) e representam unidades intercambiáveis de um mesmo ativo; NFTs são unidades únicas, usadas para identificar itens específicos.

Exemplo: Um token ERC-20 pode representar saldo de uma stablecoin; um NFT pode representar um ingresso individual para um evento.

Transação (Tx)

Qualquer operação registrada na rede, seja envio de valor entre carteiras, seja interação com um contrato inteligente ou protocolo DeFi.

Exemplo: Cada vez que você aprova um swap em uma DEX, uma nova transação é criada e gravada na blockchain.

Tx Hash (ID da transação)

Identificador único, composto por uma longa sequência de caracteres, que funciona como 'número de protocolo' de uma operação na blockchain.

Exemplo: Para documentar o caso no inquérito, é fundamental registrar o hash das transações em que houve a saída dos valores.

2. RISCO & GOLPES (A–Z)

Address Poisoning

Envio de pequenas transações para 'poluir' o histórico de endereços e induzir a vítima a copiar endereço errado em transferências futuras.

Exemplo: Golpista envia 0.001 ETH para sua carteira com endereço similar ao seu para confundir.

Airdrop/Mint Falso

Promessa de tokens grátis ou NFTs exclusivos que leva a sites maliciosos que drenam a carteira após assinatura.

Exemplo: Site falso promete airdrop de 1000 tokens USDT, mas drena tudo após você conectar a MetaMask.

Approve / Token Approval

Permissão que autoriza um contrato a gastar uma quantidade específica de tokens da sua carteira.

Exemplo: Ao usar uma DEX, você dá 'approve' para o contrato gastar no máximo 1000 USDT do seu saldo.

Bridge/DEX Clone

Cópia exata de sites famosos (Uniswap, bridges) em URLs ligeiramente diferentes para roubar aprovações ou fundos.

Exemplo: Uniswap[.]finance ao invés de uniswap.org - drena carteira em segundos.

Drainer

Contrato malicioso que limpa todos os ativos da carteira assim que o usuário assina uma permissão.

Exemplo: dApps falsas usam drainers que transferem ETH, USDT e todos os tokens aprovados em uma única transação.

Exchange Falsa

Plataforma que simula corretora real, recebe depósitos mas bloqueia saques indefinidamente.

Exemplo: Vítima deposita 10 ETH em exchange falsa que mostra saldo mas nunca libera saque.

Honeypot Token

Token que permite compra mas bloqueia venda, prendendo fundos da vítima no contrato.

Exemplo: Token novo sobe 1000%, mas quando você tenta vender, a transação falha por design.

Ice Phishing

Técnica em que vítima é convencida a assinar transação que altera permissões, permitindo roubo posterior.

Exemplo: Site pede assinatura 'sem gas' que na verdade dá permissão infinita para o contrato do golpista.

Malware de Clipboard

Vírus que substitui endereço copiado pelo do golpista no momento em que você cola.

Exemplo: Você copia endereço legítimo, mas malware troca por endereço do criminoso no Ctrl+V.

Permit / Assinatura 'sem gas'

Autorização feita apenas por assinatura digital que permite movimentação posterior dos fundos.

Exemplo: dApp pede 'permit' para gastar USDT sem pagar gas na hora - golpista usa depois.

Phishing

Engano por meio de sites, emails ou anúncios falsos que imitam serviços legítimos para roubar dados.

2. RISCO & GOLPES (A–Z) — continuação

Phishing (cont.)

Exemplo: Email falso da Binance pedindo verificação de conta leva a site que rouba login/senha.

Pump and Dump

Inflação artificial de preço para atrair vítimas, seguida de venda massiva pelos organizadores.

Exemplo: Grupo de Telegram promove token que sobe 5000% em 2 horas, depois cai 99%.

Recovery Scam

Golpe que promete recuperar cripto perdida mediante pagamento antecipado de 'taxas'.

Exemplo: Após vítima perder 5 ETH, 'especialista' promete recuperar por 20% do valor adiantado.

Rug Pull

Desenvolvedores retiram liquidez ou fogem com fundos dos investidores.

Exemplo: Projeto DeFi levanta US$10M, desenvolvedores somem e token vira pó.

SIM Swap

Sequestro do número de celular para burlar autenticação SMS e resetar senhas.

Exemplo: Golpista convence operadora a transferir chip da vítima para seu SIM card.

Suporte Falso

Golpistas se passando por 'suporte oficial' em Telegram/WhatsApp para roubar seed ou códigos.

Exemplo: Telegram falso da MetaMask pede sua seed phrase para 'resolver problema de conexão'.

Unlimited Approval

Autorização que permite gasto infinito de um token por um contrato.

Exemplo: Aprovação infinita de USDT permite que contrato malicioso esvazie toda a carteira.

Wash Trading

Negociação consigo mesmo para inflar volume artificialmente.

Exemplo: Exchange cria volume falso de R$1B/dia negociando consigo mesma.

3. SEGURANÇA (A–Z)

2FA / MFA

Autenticação adicional além da senha, usando app autenticador ou chave física.

Exemplo: Google Authenticator gera código de 6 dígitos que muda a cada 30 segundos.

Backup Seguro

Armazenamento da seed phrase em papel/metal em local físico seguro.

Exemplo: Seed gravada em placa de aço fica imune a incêndio e roubo digital.

Hardware Wallet

Dispositivo físico que mantém chaves privadas offline.

Exemplo: Ledger ou Trezor assinam transações sem expor chaves à internet.

Higiene Digital / OPSEC

Práticas para minimizar exposição digital e riscos de segurança.

Exemplo: Usar navegador dedicado apenas para cripto, sem extensões desnecessárias.

Hot Wallet vs Cold Wallet

Hot: conectada à internet (conveniente mas arriscada).
Cold: offline (segura mas menos prática).

Exemplo: MetaMask é hot wallet; Ledger é cold wallet.

Lista Branca (Whitelist)

Restringir saques apenas para endereços previamente aprovados.

Exemplo: Corretora permite saque apenas para 3 endereços cadastrados pelo usuário.

Revogar Aprovações (Revoke)

Cancelar permissões anteriormente dadas a contratos inteligentes.

Exemplo: Revoke.cash mostra todas as aprovações ativas e permite cancelar com um clique.