

24/02/2025 aprox. às 10:00am

**BTC** a aprox. 95588.00 USD | 546543.00 BRL | **(-0.58% em 7d)**

**ETH** a aprox. 2673.13 USD | 15284.22 BRL | **(0.50% em 7d)**

**SOL** a aprox. 158.46 USD | 906.01 BRL | **(-15.79% em 7d)**

**Market Cap Criptoativos:** 3.25 tri USD | **(-2.25% em 7d)**

**Market Cap BTC:** 1.89 tri USD **(-0.53% em 7d)** | Domínio BTC 58.30% **(1.77% em 7d)**

**Market Cap ETH:** 322.20 bi USD **(0.52% em 7d)** | Domínio ETH 9.91% **(2.84% em 7d)**

**Market Cap SOL:** 77.67 bi USD **(-15.45% em 7d)** | Domínio SOL 2.39% **(-13.50% em 7d)**

**Total Value Locked em DeFi:** 195.71 bi USD **(-1.90% em 7d)**

**DEX vs CEX dominância:** 33.37% **(13.15% em 7d)**

### **Principais eventos da semana (Horário de Brasília):**

- **Segunda-feira, 24 de fevereiro de 2025**  
05:00 – Alemanha: Índice IFO de clima de negócios (Fevereiro).
- **Terça-feira, 25 de fevereiro de 2025**  
12:00 – EUA: Índice de confiança do consumidor do Conference Board (Fevereiro).
- **Quarta-feira, 26 de fevereiro de 2025**  
12:00 – EUA: Vendas de novas casas (Dezembro).
- **Quinta-feira, 27 de fevereiro de 2025**  
05:00 – Zona do Euro: Oferta monetária M3 (Janeiro).  
10:30 – EUA: PIB do 4º trimestre (2ª estimativa).  
12:00 – EUA: Pedidos de bens duráveis (Janeiro, 1ª estimativa).
- **Sexta-feira, 28 de fevereiro de 2025**  
10:30 – EUA: Renda e gastos pessoais, incluindo PCE (headline e core) – Janeiro.  
11:45 – EUA: PMI de Chicago (Fevereiro).

## Os riscos de custódia em cripto

**Caros(as) amigos e amigas,**

No fim do último dia útil da semana, por volta das 15:30 do horário de Brasília, foi confirmado pelos executivos da Bybit um hack envolvendo valores que chegam a **mais de US\$ 1 bilhão**, sendo o alvo uma *cold wallet* que continha um pouco mais de **400 mil ETH**. Isso demonstra o risco associado à custódia em cripto e como a segurança em cripto é algo muito importante, sempre sendo um tópico ressaltado e fortalecendo ainda mais as necessidades regulatórias claras. **Na Análise da Semana** destrinchamos com maiores detalhes o maior hack da história envolvendo cripto, pontuando os principais pontos em relação ao evento.

Porém, a semana começou ainda com as repercussões da irresponsável ação do Milei e da memecoin Libra. O feriado do **Presidents Day** nos EUA, de certa forma, manteve o **Bitcoin** na faixa dos **US\$ 96 mil**, mas, com a reabertura do mercado na terça-feira, o principal criptoativo caiu para a casa dos **US\$ 93 mil**.

Já comentamos que essa febre das **memecoins** traz, em parte, um aspecto muito perigoso do mercado de criptoativos. Não devemos vê-lo como um cassino, mas sim como um investimento de longo prazo em uma tecnologia inovadora. Por outro lado, a proliferação das memecoins mostra como ainda estamos em uma fase muito inicial desse mercado e como a tecnologia blockchain continua explorando novas possibilidades na sociedade.

Em linhas breves, o [governo Milei](#) recuou na proposta de lançar a **Libra**, um token lastreado no peso digital, após denúncias de que insiders lucraram cerca de **US\$ 87 milhões** antes do anúncio oficial da reversão. O projeto, que prometia eficiência e integração ao dólar, rapidamente se tornou alvo de críticas por falta de governança e transparência, levantando dúvidas sobre a coerência da política econômica do governo, especialmente diante da inflação anual de **211%** na Argentina. O episódio escancarou a fragilidade regulatória e reforçou como, sem regras claras, tokens podem ser usados para especulação e enriquecimento de poucos. No mercado, o peso argentino seguiu pressionado, enquanto ativos cripto no país registraram alta volatilidade.

A investigação revelou o envolvimento de diversas plataformas **DeFi** no ecossistema **Solana**, incluindo **Meteora**, **Jupiter**, **DefiTuna** e o mecanismo de staking **M3M3**. **Hayden Davis**, CEO da **Kelsier Ventures**, foi apontado como o responsável pelo lançamento da **Libra** e exposto por manipulação de mercado, não apenas com esse token, mas também com **\$MELANIA** e **M3M3**. A crise levou à renúncia de **Ben Chow**, fundador da **Meteora**, após se revelar que ele sabia do golpe, mas não interveio devido à pressão da **Kelsier**.

Este é mais um episódio que pode levar a um aumento na fiscalização sobre outros projetos cripto, especialmente agora que uma força-tarefa nos **EUA** está focada nesse mercado.

Mais um evento que demonstra que blockchain não é o problema, mas sim o que tentam fazer com ela. Como é o caso que já vimos acontecer com a internet diversas vezes.

Além do “micro-cripto”, também tem o macro.

No dia 19, o Federal Reserve divulgou a ata da reunião de janeiro do Comitê de Política Monetária (FOMC), confirmando o que o mercado já esperava. O documento reiterou a abordagem cautelosa do banco central, enfatizando que os cortes de juros só serão considerados quando houver sinais mais claros de controle da inflação. Além disso, os membros do comitê expressaram preocupações de que mudanças nas políticas comercial e de imigração poderiam aumentar os riscos inflacionários. Empresas relataram ao banco central que pretendem repassar aos consumidores os custos adicionais resultantes das tarifas de importação propostas pelo governo Trump. Essas potenciais alterações foram vistas como fatores que poderiam dificultar o processo de desinflação nos EUA.

O mercado reagiu positivamente à previsibilidade da comunicação do Fed: o S&P 500 renovou seu recorde pelo segundo dia consecutivo. Esse desempenho impressionante do S&P persiste mesmo com as incertezas políticas em Washington, que acabaram sendo ignoradas pelo mercado, que preferiu se apegar à sensação de estabilidade oferecida pelo banco central.

O próximo encontro do FOMC será em 19 de março, mas, por ora, um corte na taxa de juros parece provável apenas a partir de julho.

Enquanto isso, Trump voltou a sugerir um novo acordo comercial com a China, prometendo um escopo ainda mais amplo do que o firmado em seu primeiro mandato. Segundo ele, esse pacto incluiria não só investimentos e ampliação das compras chinesas de produtos americanos, mas também temas de segurança nuclear. O mercado, no entanto, recebe essas declarações com ceticismo. Trump tem um histórico de falas infladas e posicionamentos voláteis e, por ora, as tarifas de 10% sobre produtos chineses seguem em vigor. Ainda assim, apenas a sinalização de que a relação entre as duas maiores economias do mundo pode caminhar para um novo entendimento já foi suficiente para reduzir parte da incerteza global e favorecer a valorização dos ativos chineses. A Alibaba, por exemplo, é um bom termômetro desse movimento: só em fevereiro, a gigante do e-commerce adicionou US\$ 123 bilhões ao seu valor de mercado, refletindo o otimismo crescente com as políticas econômicas mais robustas do governo chinês.

**Musk também segue ativo no cenário econômico, agora com o "dividendo DOGE".** A proposta, que nasceu nas redes sociais e foi levada à Casa Branca por Elon Musk, foi acolhida por Trump. O plano prevê que, ao economizar **US\$ 2 trilhões** no orçamento federal, **20%** desse valor seria destinado ao pagamento de **cheques de US\$ 5.000** para cada uma das **79 milhões de famílias americanas que pagam imposto de renda federal**. O restante seria utilizado para reduzir a dívida pública, alinhando-se à meta principal do **DOGE** de conter o déficit fiscal, controlar a inflação e, conseqüentemente, diminuir as taxas de juros. Além de estimular a economia, essa iniciativa incentivaria os cidadãos a denunciarem desperdícios e fraudes nos gastos públicos. Embora **Musk** reconheça que a meta é ambiciosa, ele destaca que, com cortes anuais de **US\$ 200 bilhões** ao longo de uma década, o objetivo pode ser alcançado.

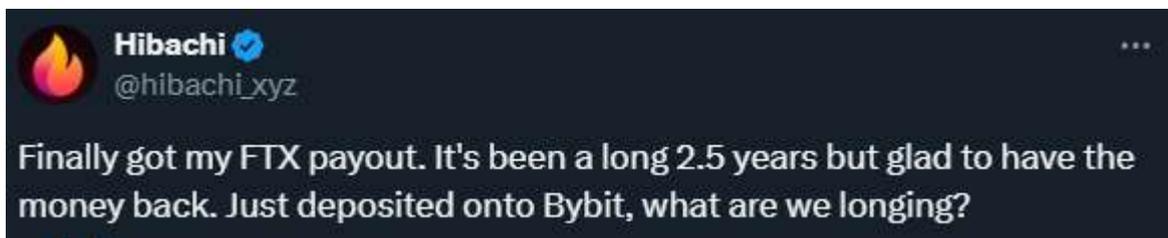
Do outro lado do mundo, Zelensky afirmou que está disposto a negociar o fim da guerra na Ucrânia, e até mesmo renunciar, se isso garantir a paz ou facilitar a entrada do país na OTAN. Às vésperas do terceiro ano do conflito, ele demonstrou abertura para um acordo com os EUA, incluindo a partilha de 50% dos recursos naturais ucranianos em troca de

garantias de segurança. Também sugeriu que os territórios ocupados pela Rússia poderiam ser incluídos na negociação, desde que a soberania e a dignidade da Ucrânia sejam preservadas.

Por fim, dois grandes eventos marcaram o setor cripto nesta semana, além do impacto do caso Milei.

O primeiro foi o [início dos pagamentos da FTX](#), que anunciou a devolução de 116% dos fundos para 98% dos usuários. No entanto, os valores serão pagos com base na cotação de novembro de 2022, resultando em US\$ 19.000 por Bitcoin (-78%), US\$ 1.300 por Ethereum (-55%) e US\$ 14 por Solana (-89%). Na prática, os investidores receberão muito menos do que seus ativos valem hoje, reforçando os riscos da custódia em plataformas não reguladas e a importância de alternativas institucionais como ETFs e fundos de investimento.

O segundo grande evento foi o maior hack do mercado cripto até o momento, que, conforme já mencionamos, dedicamos nossa análise da semana para isto.



@hibachi\_xyz sendo irônico

Fonte: Twitter

## Análise da Semana: Bye Bye Bybit?

A **Bybit**, uma das maiores corretoras do setor, foi alvo de um ataque coordenado. Um grupo de hackers — possivelmente vinculado ao **Lazarus Group**, da Coreia do Norte — conseguiu acesso a uma **cold wallet** da plataforma, desviando aproximadamente **402 mil ETH**, além de unidades de **stETH (staked ETH)**, para endereços desconhecidos. O prejuízo total estimado ultrapassou **US\$ 1,5 bilhão**, tornando-se **o maior hack da história do setor cripto**, superando em mais do que o dobro o segundo maior ataque já registrado.

Momentos antes do incidente, o Bitcoin estava em recuperação, rompendo os US\$ 99 mil, refletindo a força da narrativa positiva para o ativo neste semestre, impulsionada por um contexto macroeconômico mais favorável. No entanto, com a confirmação do hack, o preço do BTC recuou para níveis abaixo de US\$ 96 mil, refletindo o temor de que o impacto do ataque pudesse gerar novas quedas ao longo do fim de semana. O efeito sobre altcoins foi ainda mais acentuado, com tokens de menor capitalização demonstrando altos níveis de volatilidade. Ethereum, diretamente envolvido no ataque, registrou uma queda de quase 8% em poucas horas, afetado pela venda massiva dos ETHs roubados.

O ataque foi realizado explorando smart contracts, os contratos programáveis que regem as transações na blockchain. Segundo Ben Zhou, CEO da Bybit, os hackers conseguiram modificar um contrato vinculado a uma *cold wallet*, ocultando o destino final dos fundos. Isso evidencia não apenas a sofisticação do ataque, mas também um conhecimento profundo do funcionamento do *multi-sig* da plataforma.

Como já mencionamos, as investigações iniciais apontam para a atuação do **Lazarus Group**, coletivo hacker ligado ao governo norte-coreano, conforme indicam análises da **Arkham Intelligence**. Há também suspeitas de que esse mesmo grupo esteja envolvido em operações de **lavagem de dinheiro e fraudes**, utilizando plataformas como a Pump.fun para movimentar os ativos desviados. Especialistas do setor, como [ZachXBT](#), divulgaram evidências de movimentações suspeitas de carteiras associadas ao ataque, reforçando essa hipótese. Como resposta, a Tether e demais projetos, como Avalanche, THORChain e CoinEx, conseguiram bloquear cerca de **US\$ 42 milhões** relacionados ao hack, confirmando a eficácia das análises conduzidas pela comunidade e projetos reacionados ao ecossistema cripto.

Outro nome importante a se manifestar foi Changpeng Zhao (CZ), ex-CEO da Binance, [que comentou o caso em sua conta no X](#) (antigo Twitter). CZ destacou a crescente sofisticação dos ataques multi-sig, onde hackers conseguem manipular interfaces para disfarçar transações fraudulentas. Segundo ele, o incidente da Bybit reforça a necessidade de medidas preventivas mais rigorosas, incluindo pausas temporárias nos saques para mitigar danos e identificar vulnerabilidades. Ele também elogiou a postura do CEO da Bybit, enfatizando que a transparência na comunicação é essencial para manter a confiança dos usuários, especialmente diante do avanço das táticas utilizadas por grupos como o Lazarus.

Apesar da gravidade do ataque, a resposta da **Bybit** demonstrou transparência e resiliência. A corretora **não bloqueou os saques** e processou mais de **US\$ 4 bilhões** em retiradas nas **24 horas seguintes ao ataque**. No pico da crise, foram registrados **350 mil pedidos de saque**, todos atendidos sem relatos de falhas. Isso só foi possível graças à tecnologia open-source que sustenta o setor cripto, permitindo que a rastreabilidade das transações fosse conduzida de maneira eficiente por meio da blockchain. Esse nível de transparência reforça um dos principais pilares da descentralização: a possibilidade de monitorar todas as movimentações publicamente e em tempo real.

Em uma ação inédita para mitigar os danos do ataque, a Bybit anunciou uma recompensa equivalente a 10% do valor roubado para qualquer pessoa que ajudar na recuperação dos fundos desviados.

Complementando a resposta às incertezas do mercado, desenvolvedores da Ethereum reforçaram que, devido à natureza imutável da blockchain, não há possibilidade técnica de um rollback (reversão das transações já confirmadas). Qualquer tentativa de anular um hack dessa magnitude comprometeria a integridade do sistema e criaria um risco moral severo, prejudicando a confiança na descentralização da rede. Ainda assim, a comunidade cripto segue mobilizada, rastreando carteiras e explorando formas de mitigar o impacto do ataque.

Esse caso também reforça um alerta recorrente: **as exchanges centralizadas oferecem praticidade, mas impõem riscos significativos de custódia. ETFs de criptomoedas, por outro lado, operam sob rigorosas normas regulatórias, com custódia realizada por**

**instituições certificadas**, sujeitas a altos padrões de auditoria e segurança — bem diferente do ambiente pouco regulado de grande parte do setor cripto.

Por isso, sempre reforçamos a importância de **analisar com cautela qualquer corretora antes de utilizá-la**. Um evento dessa magnitude pode desencadear efeitos em toda a cadeia envolvida, afetando não apenas a plataforma atacada, mas também usuários, parceiros e outras instituições que operavam sob a mesma estrutura não regulada.

Na **QR Asset**, seguimos um dos mais rigorosos padrões de custódia do mercado, aprovados tanto pelo regulador norte-americano quanto pelo brasileiro. Nosso compromisso é garantir a **melhor solução de custódia para grandes investidores**, trazendo esse nível de segurança para o público brasileiro em geral. Este é o quarto grande evento negativo envolvendo custódia em cripto e em nenhum dos casos a QR foi afetada.

Um abraço,

**QR Asset.**