BIP 110 do Bitcoin

Reduced Data Temporary Softfork: Descrição, Questões Polémicas e Análise de Riscos/Benefícios

Resumo

A BIP 110 — Reduced Data Temporary Softfork — é uma proposta de soft fork temporário de consenso no protocolo Bitcoin, apresentada em dezembro de 2025 por Dathon Ohm e atualmente em estado Draft (fevereiro de 2026). Propõe impor, durante cerca de um ano, restrições estritas ao armazenamento de dados arbitrários não monetários nos blocos (ex.: inscrições Ordinals, Runes), limitando tamanhos de scriptPubKey (≤34 bytes, exceto OP_RETURN até 83 bytes), witness, control blocks Taproot e certos opcodes, preservando casos de uso monetários padrão. O objetivo é mitigar o impacto do "spam" on-chain na descentralização dos nós, nas taxas de transações monetárias e nos incentivos de desenvolvimento, reforçando o Bitcoin como dinheiro digital.

A medida é temporária, reversível e ativa-se via sinalização com limiar reduzido de 55 % (UASF-style).A proposta gerou forte polémica na comunidade, com oposição significativa de figuras como Adam Back, Jameson Lopp, Wang Chun e Matt Odell, que criticam o limiar baixo (risco de chain split), a introdução de censura subjetiva, o precedente perigoso para a imutabilidade, as limitações à inovação (ex.: Taproot) e a ineficácia técnica demonstrada por contornamentos rápidos.Apesar do apoio limitado (cerca de 2–7,5 % dos nós via Bitcoin Knots em fevereiro de 2026), sem sinalização relevante de mineradores, a BIP 110 permanece sem consenso suficiente para ativação iminente (prevista para ~setembro de 2026 se aprovada), representando um debate central sobre o equilíbrio entre minimalismo monetário e abertura a usos de dados no Bitcoin.

1. Introdução

As Bitcoin Improvement Proposals (BIPs) constituem o mecanismo formal de proposta, discussão e documentação de alterações ao protocolo Bitcoin. Publicadas no repositório oficial bitcoin/bips no GitHub, as BIPs abrangem desde alterações de consenso até melhorias de processos ou formatos de dados. A BIP 110, intitulada Reduced Data Temporary Softfork (também referida como RDTS, com protótipo na BIP 444), é uma proposta de soft fork de consenso, temporária, apresentada em dezembro de 2025 pelo developer Dathon Ohm (com discussão em bitcoindev).

Encontra-se no estado Draft e visa limitar, temporariamente, o armazenamento de dados arbitrários no nível de consenso, com

o objetivo declarado de proteger a função primordial do Bitcoin como dinheiro digital nativo da Internet.
A proposta foi motivada pelo crescimento exponencial de técnicas de inscriptions (iniciadas em 2022 com o protocolo Ordinals) e protocolos como Runes, que incorporam imagens, texto e outros dados não monetários nos blocos, gerando carga adicional nos operadores de nós e distorcendo incentivos de desenvolvimento.

2. Descrição Técnica da BIP 110

A BIP 110 introduz regras adicionais de validação de blocos durante um período temporário de aproximadamente um ano (52 416 blocos). Estas regras são aplicadas apenas a outputs criados após a ativação; os inputs que gastam UTXOs pré-ativação ficam permanentemente isentos. Após a expiração, todas as restrições são automaticamente removidas.

Regras de Consenso Adicionais (durante o período de ativação):

1. Os novos scriptPubKeys com mais de 34 bytes são inválidos, exceto se o primeiro opcode for OP_RETURN, caso em que até 83 bytes são permitidos.
2. Os payloads de OP_PUSHDATA e elementos da witness stack superiores a 256 bytes são inválidos (com exceção do redeemScript push em scripts BIP-16).
3. A despesa de versões de witness indefinidas (não Witness v0/BIP 141 nem Taproot/BIP 341 ou P2A) é inválida (a criação de outputs com tais versões permanece válida).
4. Witness stacks com anexo Taproot são inválidos.
5. Control blocks Taproot superiores a 257 bytes (árvore de Merkle com 128 folhas de script) são inválidos.
6. Tapscripts que incluam opcodes OP_SUCCESS em qualquer ponto (mesmo não executados) são inválidos.
7. Tapscripts que executem a instrução OP_IF ou OP_NOTIF (independentemente do resultado) são inválidos.

Estas restrições visam invalidar os principais vetores de incorporação de dados contíguos > 256 bytes, restaurar o limite histórico de 83 bytes no OP_RETURN e limitar formatos de scriptPubKey e Taproot abusados quase exclusivamente para armazenamento de dados não monetários. A proposta preserva explicitamente todos os casos de uso monetários conhecidos (pagamentos P2PKH, P2SH, SegWit, Taproot key-path spends, multisig padrão, etc.).

Mecanismo de Ativação e Desativação

- Sinalização inicia a 1 de dezembro de 2025 (bit 4 na versão de bloco). Limiar de 55 % para early lock-in (mecanismo UASF-style).
- Lock-in obrigatório previsto para cerca de agosto de 2026 (rejeição de blocos não sinalizadores).
- Ativação duas semanas após o lock-in.
- Expiração automática após ~1 ano, restaurando o estado anterior sem necessidade de novo soft fork.

A implementação está disponível em nós Bitcoin Knots e distribuições derivadas (Start9, Umbrel, myNode, etc.), permitindo sinalização opcional pelos operadores de nós.

3. Questões Polémicas Geradas pela BIP 110

A proposta gerou uma das maiores divisões na comunidade Bitcoin desde o debate SegWit (2017), com forte oposição de figuras históricas (“OGs”) como Adam Back (CEO da Blockstream), Jameson Lopp (co-

fundador da Casa), Wang Chun (co-fundador da F2Pool) e Matt Odell.

Os principais pontos de controvérsia são:

- Limiar de ativação de 55 %: Considerado excessivamente baixo face à norma histórica de 95 % (BIP 9). Críticos argumentam que constitui uma "mob rule" ou "ataque de maioria" que pode forçar uma bifurcação de cadeia sem consenso amplo, violando o princípio de governação descentralizada do Bitcoin.
- Risco de chain split: Ao rejeitar blocos não conformes (diferente de soft forks anteriores, que os aceitavam), cria potencial para duas cadeias concorrentes. Sem proteção contra replay, o ecossistema poderia paralisar.
- Ataque à neutralidade e imutabilidade: A restrição seletiva de dados é vista como censura subjetiva ("spam" vs. "dados legítimos"), enfraquecendo a resistência à censura e abrindo precedente perigoso para futuras intervenções.
- Conflito com inovação: Restrições ao Taproot (anexos, OP_IF, control blocks) limitam contratos inteligentes avançados (ex.: BitVM) e ferramentas como Miniscript, forçando upgrades futuros a hard forks.
- Ineficácia técnica: Demonstrou-se que é possível contornar as limitações (ex.: Peter Todd incorporou o texto completo da BIP numa transação conforme), iniciando um jogo do gato e do rato sem resolver o problema de fundo.
- Narrativa de "proteção infantil" e regulação: Alguns proponentes associaram o "spam" a conteúdo ilegal (CSAM); opositores consideram esta retórica perigosa, pois atrai escrutínio regulatório e sugere que o protocolo pode ser alterado por pressão externa.

A discussão transcendeu fóruns técnicos (bitcoindev, Reddit, X/Twitter) e envolveu mineradores, exchanges e investidores institucionais, com acusações mútuas de centralização e de "ataque à reputação do Bitcoin".

4. Riscos e Benefícios da BIP 110

Benefícios

- Redução de carga nos operadores de nós: Limita o crescimento do conjunto UTXO (armazenado em memória rápida e dispendiosa) e o volume de dados não podáveis, melhorando a descentralização e baixando o custo de execução de nós completos.
- Correção de incentivos distorcidos: Elimina a competição desleal entre transações monetárias e armazenamento de dados, reduzindo taxas para utilizadores normais e desencorajando a dependência de processadores de pagamento de terceiros (mais susceptíveis a censura).
- Foco no propósito monetário: Envia uma mensagem clara de que o Bitcoin prioriza "fazer uma coisa e fazê-la bem", libertando recursos de desenvolvimento de scope creep.
- Medida temporária e reversível: Permite avaliação empírica durante um ano, com possibilidade de refinamento ou abandono sem alterações permanentes.
- Preservação total de casos de uso monetários: Não afeta pagamentos, Lightning Network, multisig ou Taproot key-path spends.

Riscos

- Risco elevado de bifurcação de cadeia: Com limiar baixo e oposição significativa de mineradores (F2Pool e outros), pode ocorrer split com consequências económicas graves (incerteza, double-spend, paralisação de exchanges).
- Congelamento potencial de fundos: Embora mitigado pelas isenções pré-ativação e período de graça, edge cases em wallets experimentais ou pré-assinadas podem tornar UTXOs, temporariamente, não gastáveis.
- Precedente perigoso: Introduz censura subjetiva no consenso, enfraquecendo a narrativa de imutabilidade e abrindo porta a intervenções futuras (slippery slope).
- Restrição à inovação: Limita funcionalidades Taproot e hooks de upgrade, podendo atrasar projetos como BitVM ou novos soft forks durante o ano de vigência.
- Complexidade operacional (ainda que) temporária: Criação de dois conjuntos de regras (pré e pós-expiração), exigindo atualizações de wallets e aumentando risco de erros humanos ou bugs não detetados.
- Riscos regulatórios: Pode ser interpretado como admissão de que o Bitcoin "pode ser corrigido" por pressão comunitária, convidando intervenções governamentais.
- Ineficácia a longo prazo: Não impede esteganografia nem spam futuro; pode apenas deslocar o problema para outras técnicas ou cadeias alternativas.

5. Conclusão e Estado Atual

A BIP 110 representa uma tentativa radical de reafirmar a visão "Bitcoin como dinheiro" contra o uso crescente como armazenamento de dados arbitrários. Embora tecnicamente simples e com benefícios claros para a descentralização e eficiência monetária, os riscos de divisão da cadeia, perda de neutralidade e restrição à inovação são substanciais e têm sido amplamente contestados por líderes históricos da comunidade.

A proposta permanece em estado Draft, com sinalização ativa em nós Bitcoin Knots (percentagem variável, tipicamente < 5 % do total de nós reportados). A sua adoção depende de consenso minerador e económico; sem apoio maioritário, é provável que expire sem ativação ou que resulte em fork minoritário de curta duração. Recomenda-se aos utilizadores e desenvolvedores acompanhar a discussão oficial em bitcoindev e no repositório GitHub para atualizações em tempo real.