BitNote: Bitcoin como Nota Fisica

Bearer Assets Off-Chain com Secure Elements e Criptografia Pos-Quantica

Autor: bitnote-official
Data: 13 de novembro de 2025
GitHub: github.com/bitnote-official/bitnote
Site: bitnote.org (em construcao)
Licenca: MIT - Use, modifique, fabrique, venda livremente
Timestamp Blockchain: [a ser aplicado via OpenTimestamps]

---

1. Resumo Executivo

O **BitNote** e um dispositivo fisico open-source que transforma **Bitcoin em dinheiro de bolso real**:

- **50-100 chaves privadas independentes** (nao derivadas de uma seed)
- Cada chave pre-carregada com **2.500 satoshis** (~$2,50 em 13/11/2025)
- Transferencia **local via NFC** (sem internet, sem taxa, sem blockchain)
- **Apagamento irreversivel** no emissor apos transferencia
- **100% nao-custodial, 100% off-chain, 100% privado**
- **Criptografia pos-quantica (PQC)** integrada desde o firmware

Objetivo: Viabilizar **troco fisico em Bitcoin** com a mesma praticidade de uma nota de papel.

---

2. Problema: Bitcoin Nao E Dinheiro de Rua

Limitacao Atual	Consequencia
Transacoes on-chain	Lentas (10-60 min), caras (>R$5), rastreaveis
Lightning Network	Requer internet, canais abertos, complexidade
Ecash (Cashu, Fedimint)	Custodial - depende de mints
Opendime	

Limitacao Atual	Consequencia
	Apenas **1 chave por dispositivo** - inviavel para troco

---

3. Solucao: BitNote

3.1. Arquitetura Fisica

Componente	Funcao	Custo
ESP32-S3	MCU com WiFi/BLE (opcional)	R$ 80
ATECC608B	**Secure Element EAL5+** - gera, armazena, apaga chaves	R$ 15
PN532	Modulo NFC 13.56 MHz	R$ 40
Bateria LiPo 500mAh	Autonomia 24h+	R$ 30
LED + Botao	Interface minima	R$ 10

> **Custo total por unidade: ~R$ 175** (producao em escala: <R$ 100)

3.2. Protocolo de Transferencia Atomica (NFC)

A (emissor) -> B (receptor):

A seleciona: [slot_3, slot_7, slot_12] -> 7.500 sats A envia via NFC: Endereco de cada slot Assinatura ECDSA/Dilithium (prova de posse) Hash do slot (anti-replay)

B verifica assinatura -> armazena no seu ATECC608B

B responde: “OK” A executa: secure_element.wipe_slot(i) -> IRREVERSIVEL LED verde: “Transferencia concluida”

> **Zero copia. Zero exposicao. Zero dupla gasto.**

3.3. Criptografia Pos-Quantica (PQC) - Obrigatoria

O BitNote **nao usa apenas ECDSA** - implementa **algoritmos NIST PQC** desde o firmware:

Camada	Algoritmo	Funcao
Assinatura	**CRYSTALS-Dilithium**	Substitui ECDSA (resistente a Shor)
Troca de Chaves	**CRYSTALS-Kyber**	Substitui ECDH
Hash	**SHA-3-256**	Pre-quantico nativo

Implementacao:
- Biblioteca: pqm4 (otimizada para microcontroladores)
- Tamanho: +2KB flash (aceitavel no ESP32-S3)
- Latencia: <50ms por assinatura (aceitavel para NFC)

Justificativa:
> Mesmo que computadores quanticos cheguem em 2030-2040, **BitNote ja esta protegido**.

---

4. Seguranca Total (Camadas)

Camada	Protecao
Fisica	Secure element tamper-proof (EAL5+)
Criptografica	PQC (Dilithium + Kyber) + ECDSA fallback
Protocolo	Wipe atomico + anti-replay
Software	Firmware assinado + atualizacoes via USB-DFU seguro
Privacidade	Nenhuma metadata, nenhum rastreio

---

5. Pre-Carregamento (Funding)

1. Usuario gera **50 enderecos** via BitNote
2. Envia **50 micro-UTXOs de 2.500 sats cada**
    - Usa **CoinJoin** ou **PayJoin** para ofuscar
    - Taxa total: ~R$ 20 (1 transacao com RBF)
3. BitNote armazena chaves no secure element
4. Pronto para uso como “pacote de notas”

---

6. Comparacao com Projetos Existentes

Projeto	**Multi-chaves**	**Off-chain**	**Nao-custodial**	**NFC**	**Wipe**	**PQC**
Opendime	1	Yes	Yes	No	Yes	No
SatsCard	1	Yes	Yes	Yes	Yes	No
Cashu	Yes (tokens)	Yes	No	Yes	No	No
Satochip	10-20	Yes	Yes	Yes	No	No
BitNote	**50-100**	**Yes**	**Yes**	**Yes**	**Yes**	**YES**

---

7. Roadmap Open-Source

Fase	**Data**	**Meta**
v0.1	Dez/2025	Prototipo funcional (2 unidades)
v0.5	Jan/2026	Firmware com PQC + testes NFC
v1.0	Mar/2026	Documentacao + PCB open-hardware
v2.0	Jun/2026	Producao comunitaria (OSHPark, JLCPCB)

---

8. Licenca e Contribuicao

Contribua:
-> github.com/bitnote-official/bitnote/issues
-> github.com/bitnote-official/bitnote/pulls

---

9. Referencias

- ATECC608B Datasheet (Microchip)
- NIST PQC Round 3 (Dilithium, Kyber)
- Opendime v4 Whitepaper
- OpenTimestamps (prova de existencia)

BitNote nao e so um dispositivo.
E o dinheiro fisico que o Bitcoin sempre quis ser.
