ANEXO I – GARGALO DA ENTREGA DE PRODUTO FÍSICO

O uso de **oráculos blockchain** pode resolver com segurança o problema da **confirmação de entrega de produtos físicos ou digitais** no PayByt. Vou te explicar de forma clara, prática e adaptada à sua plataforma:

Problema:
Em um marketplace como o **PayByt**, o pagamento em Bitcoin fica retido em uma **conta escrow**. Mas como garantir que o **produto foi realmente entregue** antes de liberar os fundos ao vendedor?

Solução: Usar Oráculos como prova de entrega
Oráculos são mecanismos que conectam dados do mundo real à blockchain. Eles podem ser usados para verificar:

- Rastreios de transportadoras (Correios, FedEx, DHL)
- Confirmações de recebimento via API
- Interações humanas via "provas de recepção" (ex: QR Code, assinatura digital)

Exemplos de como usar no PayByt:
1. Produto físico com rastreamento postal

- Ao criar o pedido, o vendedor insere o código de rastreio.
- Um **oráculo (ex: Chainlink External Adapter)** consulta a API da transportadora.
- Quando o status do rastreamento indicar "Entregue", o oráculo envia esse dado para o smart contract.
- O contrato libera automaticamente o Bitcoin ao vendedor.

Tecnologia possível:

- Chainlink + Chainlink External Adapter
- Transportadora + API (Ex: Correios, DHL, UPS)

---

2. Produto digital com chave de ativação ou entrega via link

- O vendedor envia a chave por meio da plataforma.
- O comprador deve clicar em "Recebido".
- Se não clicar após X dias, um oráculo executa uma checagem de leitura/recebimento.
- O smart contract libera os fundos.

Gatilhos extras:

- Provas de abertura (via IPFS hash)
- Provas de leitura com assinatura digital

---

3. Entrega com QR Code ou assinatura

- O comprador recebe um QR code gerado pelo contrato.
- Ao escanear com o app da transportadora ou pela própria PayByt, o oráculo recebe a confirmação.
- O smart contract libera o Bitcoin automaticamente.

Resumo da Lógica com Oráculo:

1. Compra → BTC em escrow
2. Vendedor envia produto + tracking info
3. Oráculo monitora entrega
4. Entrega confirmada = libera BTC

Ferramentas recomendadas:

- Chainlink – oráculo descentralizado com suporte a contratos inteligentes
- Band Protocol – alternativa com oráculos leves
- API3 – oráculos gerenciados por DAO
- Everest – para prova de identidade sem KYC

FLUXO TÉCNICO – PAYBYT + ORÁCULO DE ENTREGA

1. Cenário

- Produto comprado no PayByt
- Bitcoin do comprador vai para **escrow (smart contract)**
- Produto é enviado pelo vendedor
- Oráculo confirma a entrega via API externa (ex: Correios)
- Smart contract libera os fundos

---

2. Arquitetura do Fluxo

Comprador Vendedor PayByt Backend Oráculo (ex: Chainlink) Smart Contract | | | | | | Compra produto | | | | |-------->| | | | | |--> Envia código ---| | | | de rastreio | | | | | |-- Solicita status ------->| | | | | do rastreio (API) | | | |--> Confirma entrega --->| | | | |--> Libera BTC

3. Componentes Técnicos

A. Smart Contract (escrow contract)

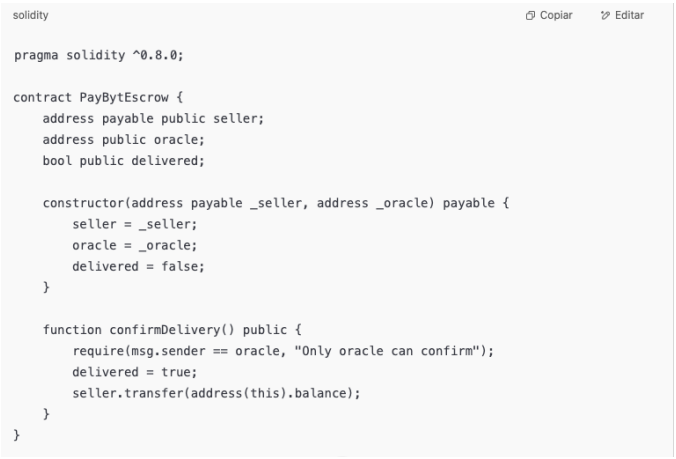
Escrito em Solidity. Simula a lógica de retenção de BTC e liberação após sinal do oráculo.

```solidity
pragma solidity ^0.8.0;

contract PayBytEscrow {
    address payable public seller;
    address public oracle;
    bool public delivered;

    constructor(address payable _seller, address _oracle) payable {
        seller = _seller;
        oracle = _oracle;
        delivered = false;
    }

    function confirmDelivery() public {
        require(msg.sender == oracle, "Only oracle can confirm");
        delivered = true;
        seller.transfer(address(this).balance);
    }
}
```

3. Componentes Técnicos

A. Smart Contract (escrow contract)

Escrito em Solidity. Simula a lógica de retenção de BTC e liberação após sinal do oráculo.



B. Oráculo (Chainlink External Adapter)

Esse oráculo será hospedado no backend do PayByt ou num nó Chainlink. Ele consulta uma **API de rastreio**, como Correios ou DHL.
Exemplo de payload esperado da API:

```json
{
  "tracking_code": "AA123456789BR",
  "status": "Entregue"
}
```

O oráculo envia o sinal para o smart contract executando a função `confirmDelivery()`.

C. Backend do PayByt

O backend:

- Recebe o código de rastreio do vendedor
- Agenda uma consulta à API de rastreio
- Monitora o status periodicamente (ex: a cada 30 min)
- Ao detectar “Entregue”, ativa o oráculo

3. Alternativas de Confirmação

- **Produto digital:** comprador assina um hash ou clica em “Recebido” → contrato valida assinatura
- **Produto com entrega presencial:** QR Code do contrato escaneado no momento da entrega

4. Tecnologias utilizadas

Componente	**Tecnologia**
Smart contract	Solidity (Ethereum / BSC / RSK / Lightning future)
Oráculo	Chainlink External Adapter
Backend API	Node.js (Express + Axios)
Blockchain	Bitcoin (Lightning para micro-pagamentos)
Banco de dados	MongoDB (para histórico)

---

6. Segurança

- Oráculo autorizado via require(msg.sender == oracle)
- Taxa da plataforma calculada no contrato (platformFee)
- Todas as ações assinadas digitalmente e registradas