Caton 微博彩 PoC 实现方案

X402 + ERC-8004 混合支付集成

📋 执行摘要

本文档整合 **X402**（支付协议）**+ ERC-8004**（信任层）到 Caton 微博彩 PoC，实现：

✅ 链上支付追踪记录 - 精确时间戳
✅ 链下法币结算 - PIX、ACH、SEPA、卡
✅ 监管合规 - 不可篡改的审计追踪
✅ 零加密风险 - 保持区块链透明度但使用法币
✅ 成本降低**95%** - 混合链上/链下架构

核心创新：区块链作为 协调层（谁、何时支付），而非结算层（价值转移）。

🏗️ 系统架构总览

混合支付流程图

用户下注（BRL巴西雷亚尔）

↓

创建并签署 X402 支付意图

↓

协调者在链上记录意图（TraceRegistry）

│ (时间戳、金额、收款方、唯一traceId)

├──→ ERC-8004 记录在 ValidationRegistry

│

↓

启动法币结算（PIX/ACH/SEPA）

│ (通过 Stripe、Nubank、本地处理器)

├─→ 结算插件将 X402 转换为法币请求

│

↓

结算处理器确认（通常 1-5 分钟 ）

│

↓

协调者在链上记录结算

│ (时间戳、法币参考哈希、追踪链接)

├─→ ERC-8004 记录在 ReputationRegistry

│

↓

授予访问权限 / 接受下注

│ (意图时临时访问，结算时完全访问)

│

↓

完整的链上审计追踪

├─→ 所有交易不可篡改

├─→ 监管机构可审计

├─→ 用户可验证支付历史

└─→ 零加密资产参与

ERC-8004 三注册表模型

```
│ • 代理可信度评分                    │
│                                    │
└────────────────────────────────────┘
```

🔧 技术实现细节

1. X402 支付协议集成

1.1 支付意图 HTTP 头

```
POST /api/bets/place HTTP/1.1

Host: caton-poc.com

Authorization: Bearer <JWT_TOKEN>

X-Payment: <X402_SIGNED_INTENT>

X-Payment-Required: 50.00 BRL

X-Payment-Reference: bet-uuid-123

X-Payment-Timestamp: 2026-01-07T22:15:30.123Z

Content-Type: application/json

{

  "market_id": "market-456",

  "amount": 50.00,

  "currency": "BRL",

  "odds": 2.50

}
```

1.2 X402 签署流程

步骤1:创建支付意图

- 用户地址、收款方、金额、时间戳

- EIP-712 结构化数据(无私钥暴露)

步骤2:签署(EIP-712)

- 用户在设备上确认

- 生成签名(SHA256)

- 签名作为支付证明

步骤3:发送到后端

- X-Payment 头中包含签名意图

- 附加原始下注数据

- 记录客户端时间戳(关键)

步骤4:后端验证

- 验证 EIP-712 签名

- 检查重放攻击(nonce)

- 提取支付细节

2. 协调者服务(后端)

协调者是 Caton 的支付处理器, 连接 X402 意图 → 法币结算。

2.1 协调者三步流程

【第1步】接收 X402 支付意图

输入:签署的支付意图头 + 下注数据

↓

1a. 验证 EIP-712 签名

1b. 生成唯一 traceId（trace-时间戳-随机）

1c. 在链上记录意图（TraceRegistry.recordIntent）

1d. 提交到 ERC-8004 验证注册表

↓ 返回给用户：临时访问权限

【第2步】启动法币结算

输入：traceId + 支付意图 + 用户支付方式

↓

2a. 确定结算处理器（PIX/ACH/SEPA/卡）

2b. 将 X402 意图转换为法币请求

2c. 提交到法币处理器（Nubank/Stripe）

2d. 返回交易 ID + 预期确认时间

↓ 时间通常：PIX 1-5分钟、ACH 1-2天、SEPA 1-2天

【第3步】结算确认（webhook）

输入：traceId + 法币交易ID + 处理器确认

↓

3a. 在链上记录结算完成

3b. 法币参考 ID 哈希存储（隐私）

3c. 提交反馈到 ERC-8004 声誉注册表

3d. 升级用户访问权限为完全访问

↓ 用户现在可以提取奖金

3. 链上追踪注册表（Solidity 合约 ）

轻量级链上合约记录支付意图和结算。

关键函数：

recordIntent(traceId, payer, payee, amount, currency, timestamp)

- 调用者：协调者

- 时机：用户提交 X402 时

- 气体成本：~2,000（Arbitrum ~$0.0001）

- 存储：最小化以节省成本

- 事件：IntentRecorded

recordSettlement(traceId, fiatReferenceHash, settlementTimestamp, status)

- 调用者：协调者

- 时机：法币处理器确认支付时

- 气体成本：~3,000（Arbitrum ~$0.00015）

- 存储：添加结算数据

- 事件：SettlementRecorded

getTrace(traceId) → PaymentTrace

- 返回完整支付生命周期数据

- 用于审计和争议解决

verifySettlement(traceId) → (isConfirmed, latency)

- 验证法币支付是否被记录

- 计算意图→结算时延

气体成本分析：

- 每笔支付总计 ~5,000 gas = **$0.00025**（Arbitrum）
- vs 传统加密支付 $1+
- 成本降低 **95%**

4. ERC-8004 集成

连接追踪注册表到 ERC-8004 注册表以建立信任。

协调者 → ERC-8004 身份注册表

- 注册为"支付协调者"

- 质押证明（例如 100 USDC）

- 支持的结算方式列表：PIX、ACH、SEPA、卡

- 司法管辖权：巴西

- 监管状态：持证

支付意图 → ERC-8004 验证注册表

- 提交验证请求（T1: 用户提交）
- 包含：traceId、金额、货币、下注 ID
- 为链下支付创建密码学证明

支付结算 → ERC-8004 声誉注册表

- 提交反馈（T2: 法币清算）
- 评分：1.0（成功）或 0.0（失败）
- 建立协调者的可信度得分
- 从上次 100 笔交易计算成功率

查询协调者声誉

- reputation_score (0.0-1.0)
- total_settlements (总数)
- success_rate (成功率%)
- recent_disputes (近期争议)

5. 可插拔结算处理器

每个法币渠道一个处理器，实现相同接口。

PIX 处理器（巴西）

processPayment(fiatRequest)

1. 验证用户 PIX 密钥（CPF/邮箱/PIX）
2. 调用 Nubank PIX API
3. 返回交易 ID + PENDING 状态
4. Webhook URL 用于确认

handleConfirmationWebhook(webhookData)

1. Nubank 确认交易完成
2. 调用 facilitatorService.confirmSettlement()
3. 更新用户访问权限

确认时间：通常 1-5 分钟（巴西即时支付系统）

ACH 处理器（美国）

processPayment(fiatRequest)

1. 验证银行账户信息
2. 通过 Plaid/Stripe 启动 ACH
3. 返回交易 ID + PENDING 状态

handleConfirmationWebhook

1. 银行确认交易
2. 调用 confirmSettlement()

确认时间：通常 1-2 个工作日

📊 工作流程：用户下注端到端流程

场景：用户下注 R$ 50 在 Flamengo vs Vasco 比赛

【T0】用户打开下注屏幕

显示：

市场："Flamengo vs Vasco"

赔率：2.50

输入下注金额：R$ 50.00

按钮："用 PIX 下注"

【T1】用户点击下注（客户端时间戳）

clientPlacedAt = "2026-01-07T22:15:30.123Z"

【T2】移动应用发送到后端（含 X402 头）

POST /api/bets/place

Headers:

X-Payment: { "amount": 50.00, "signature": "0x...", ... }

Body:

{

"market_id": "market-456",

"amount": 50.00,

"odds": 2.50,

"clientPlacedAt": "2026-01-07T22:15:30.123Z"

}

【T3】后端在链上记录意图

traceId = "trace-1673048130123-abcdef12"

调用：traceRegistry.recordIntent(

traceId,

"0x_user_address",

"0x_caton_operator",

50.00,

"BRL",

Date.now()

)

气体成本：~2,000 gas ($0.0001)

【T4】后端启动 PIX 结算

pixProcessor.processPayment({

trace_id: traceId,

amount: 50.00,

recipient_key: "0x_caton_pix_key"

})

返回：{

"transaction_id": "pix-transaction-123",

"status": "PENDING"

}

【T5】后端立即授予临时访问权限

accessControlService.grantProvisionalAccess(

userId, traceId, betData

)

返回访问令牌：10 分钟过期

【T5 响应给用户】

```
{
  "bet_id": "bet-1673048130-xyz",
  "status": "CREATED",
  "payment_status": "SETTLEMENT_INITIATED",
  "trace_id": "trace-1673048130123-abcdef12",
  "access_level": "PROVISIONAL",
  "message": "下注已接受（临时访问）。等待支付确认。",
  "expected_confirmation_time": "5 分钟"
}
```

✓ 用户现在可以查看下注和现场比赛

✗ 但不能提取奖金（等待完全访问）

【T10 (T+5分钟)】PIX 处理器确认结算

Nubank webhook 调用：

```
POST /api/webhooks/payment/confirm
{
  "trace_id": "trace-1673048130123-abcdef12",
  "fiat_transaction_id": "pix-transaction-123",
  "processor": "PIX",
  "status": "CONFIRMED"
}
```

【T11】后端在链上记录结算完成

调用：traceRegistry.recordSettlement(

traceId,

"0x_hashed_pix_reference",

Date.now(),

"CONFIRMED"

)

气体成本：~3,000 gas ($0.00015)

总成本：~5,000 gas ≈ **$0.00025**

【T12】后端升级访问权限为完全

accessControlService.grantFullAccess(userId, traceId)

返回访问令牌：30 天过期

✓ 用户现在可以：

- 提取奖金

- 进行新的下注

- 访问完整历史记录

【完整的链上审计追踪】

用户可在区块链浏览器中查看：

- 意图记录时间戳

- 结算确认时间戳

- 法币参考哈希（隐私保护）

- ERC-8004 验证链接

- 所有不可篡改的记录

🎯 核心功能特性

1. 支付追踪与审计

功能	实现	好处
支付意图记录	X402 签署 + 链上时间戳	不可否认的证明
结算追踪	法币参考哈希 + 时间戳	监管合规
争议解决	自动时间验证	降低人工成本
完整审计	链上不可篡改	监管机构可验证

2. 低延迟访问控制

阶段	时间	访问级别	可操作
意图记录	T0	PROVISIONAL	查看下注、观看直播
法币结算	T1-T2	PROVISIONAL	同上（等待确认）
结算确认	T2	FULL	提取奖金、新下注
结算失败	T+超时	REVOKED	自动退款

3. 协调者声誉系统

通过 ERC-8004：

✓ 自动构建成功率指标

✓ 公开查询协调者可信度

✓ 用户可选择高声誉的协调者

✓ 矿工可用于定价/佣金决策

好处:

- 激励诚实的结算行为

- 竞争推动成本下降

- 透明的信任信号

- 无需中央权威

🔐 关键创新点

1. 混合链上/链下架构

传统加密支付(100% 链上):

用户钱包 → 智能合约 → 交易 → 矿工费 ($1+)

问题:用户需要加密资产、波动风险、监管不清

Caton 混合方案:

用户(法币账户)

↓ X402 签署

协调者(支付追踪 → 链上记录)

↓ 法币结算 → PIX/ACH/SEPA

区块链(时间戳 + 审计 + 声誉)

优势:

✓ 用户用熟悉的法币支付

✓ 协调者成本 $0.00025（vs $1+）

✓ 完整的监管审计追踪

✓ 零加密风险

2. X402 + ERC-8004 协同

X402（支付协议）

↓

提供：客户端签署、重放保护、协调者抽象

功能：支持任何结算方式（加密、法币等）

ERC-8004（信任层）

↓

提供：身份注册、验证记录、声誉跟踪

功能：链下事件的可验证记录

结合：

1. X402 记录支付意图和授权
2. ERC-8004 验证支付确实结算了
3. 用户获得密码学证明
4. 协调者构建声誉
5. 监管机构可审计

📈 性能与成本

成本对比

传统加密支付（链上结算）

每笔交易：~200,000 gas @ Arbitrum = $0.01-0.05

Caton 混合方案

意图记录：2,000 gas = $0.0001

结算记录：3,000 gas = $0.00015

总计：5,000 gas = **$0.00025**

成本降低：95%

延迟

用户体验延迟（T0 → T5）：< 1 秒

- 移动应用签署：200ms
- 网络往返：100ms
- 后端验证 + 链上：500ms
- 返回响应：100ms

结算确认延迟（取决于法币方式）：

- PIX（巴西）：1-5 分钟
- ACH（美国）：1-2 个工作日
- SEPA（欧洲）：1-2 个工作日
- 卡：实时或 1-3 分钟

用户访问延迟：

- 临时访问（意图时）：0 秒

- 完全访问（结算确认时）：取决于上述

🚀 实现路线图

阶段 1：最小可行产品（1-2 周）

核心功能：

✓ 用户认证 + JWT

✓ X402 签署流程

✓ 链上追踪注册表（Solidity）

✓ PIX 处理器

✓ 临时访问控制

✓ webhook 确认

演示能力：

- 用户下注 → 链上记录

- 自动 PIX 结算

- 临时访问功能

- 基础指标仪表盘

阶段 2：完整 MVP（2-4 周）

新增功能：

✓ ERC-8004 集成

✓ ACH 处理器

✓ 争议解决（TEE 模拟）

✓ 用户面对面仪表盘

✓ 操作员指标仪表盘

✓ 审计日志导出

阶段 3：生产准备（4-8 周）

优化和合规：

✓ 多签协调者（高价值）

✓ SEPA 处理器（欧洲）

✓ 卡支付处理器

✓ KYC/AML 集成

✓ 实时事件流

✓ 生产监控和告警

✅ 为什么这对 Caton 有效

监管优势

巴西博彩监管要求：

✓ 支付可追踪性

✓ 反洗钱合规

✓ 不可否认的审计

✓ 即时访问控制

Caton 混合方案满足所有要求：

✓ X402 签署 = 支付证明

✓ ERC-8004 验证 = 不可篡改记录

✓ 链上时间戳 = 不可否认的事实

✓ 访问控制 = 即时合规执行

成本优势

传统微博彩系统：

支付处理：每笔 0.5-2% 手续费

欺诈管理：每笔 0.1-0.3%

争议解决：人工成本高

Caton：

支付追踪：$0.00025（气体）

自动化验证：近零成本

争议解决：自动化（时间戳）

节省：90% 以上

用户体验优势

临时访问：

- 用户立即看到接受的下注

- 可观看现场直播

- 建立信心

完全透明：

- 可在区块链查看支付证明

- 清楚的时间戳

- 纠纷时的自动化决议

熟悉支付方式：

- PIX、银行转账等

- 无需加密资产

- 风险较低

🔍 安全注意事项

威胁模型与缓解

威胁 1：协调者欺诈

→ 缓解：ERC-8004 身份注册 + 质押

多签要求（高价值）

声誉记录公开

威胁 2：法币处理器延迟

→ 缓解：临时访问立即授予

自动超时 + 退款

多备份处理器

威胁 3：链下/链上不同步

→ 缓解：确定性法币参考哈希

自动对账

监管审计日志

威胁 4：隐私泄露

→ 缓解：法币参考 ID 哈希

ERC-8004 隐私注册表

选择性披露机制

📞 关键接触点（API）

用户应用

POST /api/auth/login

→ JWT token

GET /api/events

→ 活跃事件列表

GET /api/markets/event/:eventId

→ 该事件的市场和赔率

POST /api/bets/place

Headers: X-Payment

→ 下注 ID + 支付状态

GET /api/bets/:betId

→ 完整下注详情（包括 traceId）

GET /api/traces/:traceId

→ 完整支付生命周期（链上数据）

POST /api/disputes/create

→ 争议创建 + TEE 判决

操作员仪表盘

GET /api/metrics/event/:eventId

→ 总下注、接受率、延迟、处理量、争议

GET /api/admin/facilitator/reputation

→ 协调者声誉和性能

GET /api/admin/audit-log

→ 完整的可审计交易日志

🎬 演示流程（合作伙伴演示）

【步骤 1】展示直播 + 市场

"这是现场足球比赛和实时微博彩市场"

【步骤 2】下注 + 即时反馈

点击下注 → 显示：

✓ 下注被接受（<1 秒）

✓ 支付状态：结算中

✓ 延迟：125 ms

✓ 临时访问授予

【步骤 3】展示链上证明

"所有数据都被记录到区块链"

显示：

- Arbitrum 上的 traceId

- 意图时间戳

- 区块浏览器链接

【步骤 4】模拟 PIX 确认（5 分钟后）

webhook 自动触发或手动模拟

显示：

✓ 支付确认

✓ 访问升级为完全

✓ 用户现在可提取奖金

【步骤 5】显示争议解决

"如果用户对延迟有异议..."

创建争议 → 显示 TEE 判决

"判决：CORRECT - 下注延迟 800ms 到达"

【步骤 6】展示指标和声誉

仪表盘显示：

- 100% 接受率（该演示事件）

- 平均延迟：145 ms

- 总处理量：R$ 5,000

- 争议率：0%

- Caton 协调者声誉：0.98（极佳）

【结论】

"这是实时、低成本、透明且合规的微博彩"

📝 文档和参考

核心规范

X402 Payment Protocol v2

https://www.x402.org/writing/x402-v2-launch

关键特性：

- EIP-712 签署

- 协调者抽象

- 多结算方式支持

ERC-8004 Trust Layer

https://eips.ethereum.org/EIPS/eip-8004

关键特性：

- 身份注册表

- 验证注册表

- 声誉注册表

PaymentTraceRegistry (Caton 特定)

轻量级 Solidity 合约

最小化链上存储

快速验证接口

部署目标

链：Arbitrum（主网或 Sepolia 测试网）

成本：极低（<$0.001 每笔交易）

速度：快速确认（通常 < 1 秒）

兼容性：支持任何 EVM 兼容链

🎓 术语表

术语	定义
X402	HTTP 标准支付协议，支持多种结算方式
ERC-8004	信任基础设施，为 AI 代理和支付处理器记录验证
TraceId	唯一的支付追踪标识符（trace-时间戳-随机）
Facilitator	支付处理器（Caton），连接 X402 和法币结算
临时访问	用户在意图记录时授予（等待法币确认）
完全访问	法币结算确认后授予（用户可提取）
声誉得分	0.0-1.0，基于成功结算的百分比
Webhook	法币处理器的异步确认（PIX、ACH 等）

📊 成功指标

技术 KPI：

✓ 支付追踪延迟 < 1 秒

✓ 链上记录成功率 99.9%

✓ 争议自动解决率 > 95%

✓ 气体成本 < $0.001/交易

业务 KPI：

✓ 法币结算成功率 > 99%

✓ 用户接受度（临时访问）> 90%

✓ 争议率 < 1%

✓ 协调者声誉得分 > 0.95

合规 KPI：

✓ 审计追踪覆盖 100%

✓ 时间戳准确性 ±100ms

✓ 隐私遵循 LGPD（巴西）

✓ KYC/AML 通过率 100%

版本：**1.0**
更新日期：**2026** 年 **1** 月 **7** 日
作者：**Caton** 技术团队

这是 Caton 微博彩 PoC 的完整技术和业务蓝图，使用 X402 + ERC-8004 实现低成本、合规、透明的支付和信任基础设施。