Tokenização Transparente e Segura de Certificados de Energia Renovável Usando Blockchain

Jeffson Sousa[1], Vinicius Duarte[1], Daniel Robson Pinto[1], Mauricio Pinto[1], Fabio Taniguchi[1], Ismael Ávila[1], Rodrigo Soprano[1], Anderson Parreira[1], Fernanda Jordão[1], Viviane Petito[1], Silvia Marion[1]

[1] Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPQD)
Campinas – SP – Brasil

{jcsousa, vduarte, danielp, mauriciop, fabiokt, avila_an, rsoprano,

parreira, fcjordao, vpetito, marion}@cpqd.com.br

Resumo. *A comercialização de Certificados Internacionais de Energia Renovável (I-RECs) enfrenta ameaças críticas de cibersegurança: dupla contagem de atributos ambientais, ausência de não-repúdio nas transações e superfície de ataque ampla em processos manuais de reconciliação. Este artigo relata um estudo de caso real de colaboração entre o CPQD e a Neoenergia para o desenvolvimento de uma plataforma de tokenização de I-RECs baseada em blockchain pública. A solução utiliza contratos inteligentes autônomos que automatizam o ciclo de vida dos certificados — da emissão à aposentadoria — e eliminam as vulnerabilidades do modelo manual vigente. Uma Prova de Conceito industrial executou mais de 18.000 transações em sete cenários de carga (5–40 TPS), demonstrando throughput compatível com as demandas do mercado e custo operacional por certificado abaixo de US$ 0,08 em rede pública. O relato detalha as decisões de arquitetura de segurança, os desafios de integração com os registros regulatórios brasileiros (CCEE e Instituto Totum) e as lições aprendidas na interação com a indústria.*

1. Introdução

O mercado de Certificados Internacionais de Energia Renovável (I-RECs) representa um ativo ambiental de alto valor: cada certificado atesta que 1 MWh foi produzido por fonte renovável específica [Instituto Totum 2024]. No Brasil, a CCEE registra os dados operacionais de geração e o Instituto Totum, operando o SISREC Ledger 2 sobre Hyperledger Fabric, gerencia a emissão e aposentadoria dos certificados na plataforma internacional Evident [CCEE 2023, Evident 2022].

Apesar dessa infraestrutura regulatória, o mercado secundário de I-RECs ainda depende fortemente de reconciliações manuais, e-mails de validação e planilhas de controle. Na Neoenergia um dos maiores grupos de energia do Brasil, o processo envolve nove etapas distribuídas entre cinco macrofases e múltiplos sistemas sem integração automática. Essa fragmentação gera uma superfície de ataque concreta: janelas temporais em que um mesmo certificado pode ser apresentado a múltiplos compradores (double retirement), ausência de trilha de auditoria irrefutável e risco de erros com impacto financeiro direto.

A tecnologia blockchain tem sido proposta como uma solução estrutural para esses riscos [Liu et al. 2024, Yamaguchi et al. 2021]. No entanto, as propriedades de se-

gurança das implementações de contratos inteligentes para mercados de certificados não foram formalmente analisadas no contexto regulatório brasileiro, e nenhum trabalho publicado examina as características de confiabilidade de um sistema I-REC de produção implantado no Brasil.

Este artigo relata o desenvolvimento, em colaboração entre CPQD e Neoenergia, de uma plataforma de tokenização de I-RECs baseada em blockchain pública, com foco nas decisões de cibersegurança que guiaram a arquitetura e nos resultados obtidos na PoC industrial.

2. Ameaças ao Modelo Atual: O Trilema da Confiança

Rastrear eletricidade até sua fonte renovável é intrinsecamente difícil: na rede física, energia de diferentes origens se mistura instantaneamente. Os I-RECs resolvem essa rastreabilidade por equivalência lógica, 1 certificado = 1 MWh limpo em usina específica. Contudo, a governança atual concentra-se na integridade do registro de emissão e carece de propriedades de segurança nativas para o mercado secundário.

Identificamos três ameaças críticas ao modelo atual, que denominamos Trilema da Confiança:

- **Integridade comprometida:** metadados dos certificados trafegam em e-mails e planilhas sem assinatura criptográfica, permitindo alteração de volumes de MWh sem rastro auditável;
- **Dupla contagem:** ausência de atomicidade na transferência de custódia cria uma janela temporal, de horas a dias, durante a qual o mesmo I-REC pode ser aposentado para múltiplos compradores;
- **Ausência de não-repúdio:** a aposentadoria de certificados é registrada por PDF e e-mail, documentos que podem ser negados ou contestados sem mecanismo criptográfico de prova.

Essas ameaças não são hipotéticas: casos de revenda não autorizada e erros de reconciliação com impacto financeiro foram identificados no mapeamento do processo interno da Neoenergia durante a fase de levantamento do projeto.

3. Arquitetura de Segurança

3.1. Modelo Híbrido On-chain / Off-chain

A plataforma opera como sistema híbrido deliberadamente projetado para respeitar a regulação vigente. A validação primária dos dados de geração permanece off-chain junto aos provedores regulatórios confiáveis (CCEE e Instituto Totum) — não duplicamos o registro oficial. A propriedade, negociação e queima dos certificados ocorrem inteiramente on-chain em blockchain compatível com EVM, avaliada em rede permissionada Besu/QBFT, com portabilidade para redes públicas/L2, tornando essas ações criptograficamente auditáveis e irreversíveis por qualquer participante da rede.

Essa decisão de arquitetura foi resultado direto da interação com a equipe jurídica e de compliance da Neoenergia: qualquer solução que substituísse ou contornasse os registros regulatórios oficiais seria inviável para implantação industrial. O blockchain atua, portanto, como camada de segurança sobre o processo existente, não como substituto.

3.2. Camadas de Segurança

A arquitetura representada na Figura 1 é estruturada em cinco camadas:

1. **Integração Regulatória (Off-chain):** O Manager layer aceita exclusivamente chamadas autenticadas provenientes dos registros oficiais (CCEE e Instituto Totum) antes de invocar a função de minting. Isso mitiga Ataques de Oráculo, onde dados forjados off-chain seriam injetados na blockchain para disparar emissão fraudulenta de tokens.
2. **Tokenização de Ativos (On-chain):** O padrão ERC-721 é atrelado ao ERC-1155 garantindo unicidade criptográfica por certificado e frações de MWh sem quebra de custódia. Cada token incorpora metadados invioláveis: ID único, código de projeto CCEE, data de geração e fonte energética.
3. **Mercado Descentralizado:** APIs RESTful/Web3 com controle de acesso por perfil , Marketer (emissor) e Trader (comprador corporativo), criptograficamente segregados no middleware.
4. **Interoperabilidade:** Comunicação via APIs criptografadas com a plataforma Evident, espelhando ações de emissão e aposentadoria no registro oficial internacional.
5. **Auditoria e Relatórios:** Logs imutáveis on-chain que suportam protocolos ESG (GRI, CDP, RE100) e eliminam o risco de repúdio em auditorias de conformidade.

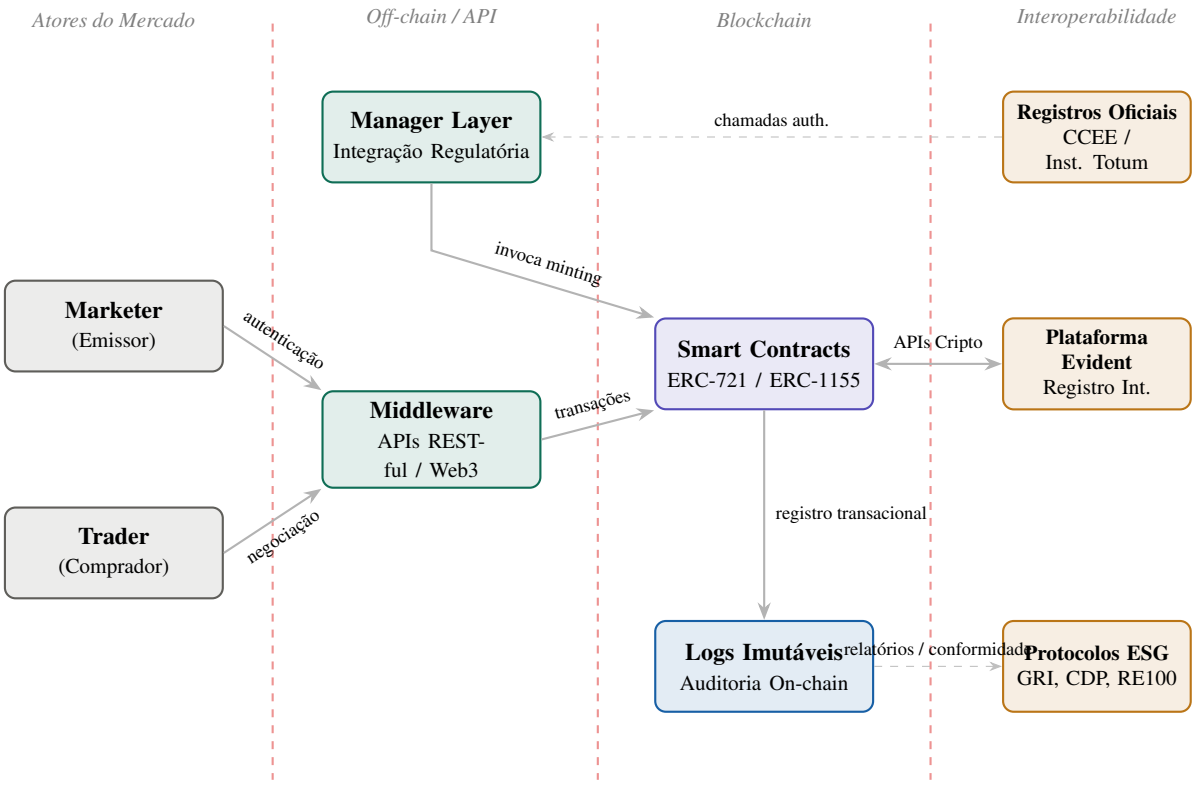

Figura 1. Diagrama de Arquitetura da Plataforma de Tokenização de Ativos Energéticos mapeando os componentes de Integração, Blockchain, Mercado, Interoperabilidade e Auditoria.

3.3. Contratos Inteligentes Autônomos

O ciclo de vida dos certificados é gerido por três contratos com responsabilidades estritamente segregadas:

- **Contrato Pre-IREC** (`AssetManager`): cofre de garantia (escrow) para energia gerada mas ainda não certificada pelo Totum. Inclui guarda de dupla emissão: um mapeamento projectId → bool impede que o mesmo projeto/período gere dois tokens distintos. Recebe dados de geração, bloqueia os ativos e aguarda confirmação de elegibilidade antes de liberar a transição de estado.
- **Contrato Certified-IREC** (`TokenIrec`): O padrão ERC-1155 permite que um mesmo contrato gerencie tokens fungíveis e semi-fungíveis: `tokenId=1` representa a NeoCoin, moeda transacional utilitária de semântica puramente fungível; cada `tokenId`≥ 2 representa um tipo de certificado I-REC. A aposentadoria é irreversível por design: a função `burnIREC` queima permanentemente a quantidade retirada e emite um evento `IRECRetired(tokenId, owner, timestamp)` que constitui prova criptográfica de irretratabilidade, auditável por qualquer nó da rede sem intermediário.
- **Contrato de Trading** (`TradeTokens`): executa trocas peer-to-peer no mercado secundário implementando o padrão Delivery versus Payment (DvP) atômico. A dedução do saldo em NeoCoins e a transferência de propriedade do token ambiental ocorrem em uma única transação indivisível. Isso elimina a janela de double retirement: não existe estado intermediário em que o I-REC tenha sido pago mas não transferido, ou transferido mas não pago.

3.4. Middleware de Gestão Criptográfica

A complexidade das chaves públicas e privadas é abstraída sem comprometer a segurança. O middleware atua como Proxy entre a aplicação web e os nós EVM (Ethereum Virtual Machine), responsável pela geração segura de sementes criptográficas, monitoramento de latência de bloco e prevenção de ataques de negação de serviço ao nível de contrato. Os nós da rede pública são isolados de exposição direta a requisições não autenticadas.

4. Resultados da Prova de Conceito

4.1. Configuração Experimental

O protótipo foi avaliado com o framework Hyperledger Caliper em sete workloads que cobrem o ciclo de vida completo dos I-RECs, com varredura de 5 a 40 TPS (200 transações por rodada, 80 execuções totais, >18.000 transações):

Tabela 1. Cargas de trabalho (*Workloads*) de referência e seu mapeamento no ciclo de vida do i-REC tokenizado

Workload	Operação	Contrato → Função
W1	Criação de NeoCoin	`TokenIrec.mintERC20`
W2	Registro de geração	`AssetManager.createPreIrec`
W3	Aquisição de pré-certificado	`AssetManager.buyPreIrec`
W4	Emissão de token (mintIREC)	`TokenIrec.mintIREC`
W5	Listagem no mercado	`TradeTokens.openIrecOffer`
W6	Compra no mercado (DvP atômico)	`TradeTokens.buyIrec`
W7	Aposentadoria (burnIREC)	`TokenIrec.burnIREC`

Tabela 2. Taxa de transferência sustentada de pico por carga de trabalho (média de rodadas repetidas no nível de TPS de melhor desempenho).

WL	Carga de Trabalho	TPS de Pico	Config. (TPS)	Eficiência
W1	MintNeocoin	26,00	35	74,3%
W2	CreatePreIrec	7,40	40	18,5%
W3	BuyPreIrec	8,10	25	32,4%
W4	MintIREC	2,92	20	14,6%
W5	OpenTradeOffer	7,58	30	25,3%
W6	BuyTradeOffer	20,90	40	52,3%
W7	BurnIREC	4,75	30	15,8%

Eficiência = TPS médio alcançado / TPS configurado.

4.2. Desempenho e Custo de Gás

A Tabela 1 mostra os cenarios de W1-W7 mostrando os TPS ótimos de cada cenario, os artefatos podem ser consultados no repositório do github[1]. O cenário W6 (buyIrec), foi observado um throughput de 21 TPS sustentado, latência média de 2,1 s. O DvP atômico não introduz overhead significativo em relação a transferências simples, resultado relevante pois confirma que a propriedade de segurança mais crítica (eliminação do *double retirement*) não compromete a usabilidade.

No cenário W4 (mintIREC), o throughput de 2,9 TPS a 40 TPS injetados, latência de até 8,0 s em pico. Operação mais custosa computacionalmente, mas compatível com a frequência real de emissão do mercado, o minting não é operação de alta frequência. Não tivemos nenhuma incidência de falha global na rede, apesar que em cenários de congestionamento extremo foi observado alta latência.

A Tabela 3 mostra a relação do custo de ciclo de vida completo de um I-REC (minting + transferência + retirement) observa-se um custo de aproximadamente 1.754.763 gas units equivalente a US$ 0,08 em Ethereum mainnet e menos de US$ 0,001 em redes L2 como Polygon.

Tabela 3. Custo acumulado de gás de um certificado I-REC durante todo o seu ciclo de vida on-chain, com projeção de custo em cadeias públicas (Mainnet do Ethereum a 15 Gwei; Polygon PoS a 30 Gwei, ETH = US$ 3.000, MATIC = US$ 0,50, valores indicativos).

WL	Fase	Contrato	Função(ões)	Frequência	Mediana (gás)	Custo (Ethereum)	Custo (Polygon)
W2	Pré-emissão	`AssetManager`	`createPreIrec`	Uma vez por lote	227.401	≈ US$ 0,010	< US$ 0,001
W3	Compra primária	`AssetManager`	`buyPreIrec`	Uma vez por comprador	231.187	≈ US$ 0,010	< US$ 0,001
W4	Emissão	`TokenIrec`	`mintIREC`	Uma vez por certificado	614.806	≈ US$ 0,028	< US$ 0,001
W5	Listagem secundária	`TradeTokens`	`openIrecOffer`	Por oferta	168.487	≈ US$ 0,008	< US$ 0,001
W6	Compra secundária	`TradeTokens`	`buyIrec`	Por execução	84.239	≈ US$ 0,004	< US$ 0,001
W7	Aposentadoria	`TokenIrec`	`burnIREC`	Uma vez (terminal)	428.643	≈ US$ 0,019	< US$ 0,001
Total do ciclo de vida completo			(W2 → W3 → W4 → W5 → W6 → W7)		**1.754.763**	**≈ US$ 0,079**	**≈ US$ 0,001**

W1 (`mintERC20`, 38.030 gás) é uma operação de tesouraria única, não incluída no total do ciclo de vida por certificado. Os preços do gás e dos tokens são ilustrativos; verifique os valores atuais antes de citá-los em contextos de comparação de custos.

A capacidade de representar frações de MWh (via ERC-1155) foi validada sem quebra de custódia do ativo matriz, habilitando um mercado secundário mais líquido que o modelo atual.

[1] `https://github.com/jeffsonsousa/irec-marketplace-evaluation`

5. Desafios e Limitações

5.1. Integração Regulatória

O maior desafio técnico não foi a implementação dos contratos inteligentes, mas a integração com os sistemas regulatórios existentes. A API da plataforma Evident não expõe endpoints para automação completa do ciclo de emissão, algumas etapas ainda requerem intervenção manual no portal. Isso impõe uma dependência off-chain que limita a automação total e representa a principal superfície de ataque residual da arquitetura atual.

Em projetos de blockchain para infraestrutura crítica regulada, a integração com os sistemas legados regulatórios é determinante e deve ser mapeada antes do design arquitetural.

5.2. Custos de Gás e Escolha de Rede

Flutuações no preço do gás em redes públicas como Ethereum mainnet introduzem imprevisibilidade de custo operacional incompatível com contratos de energia de longo prazo. A implantação em redes L2 (Polygon, Arbitrum) ou em blockchain pública permissionada compatível com EVM é necessária para produção sem comprometer a auditabilidade pública que é o diferencial da solução em relação a sistemas privados como o próprio Hyperledger Fabric do Totum.

5.3. Enquadramento Jurídico

A classificação legal dos I-RECs tokenizados como valores mobiliários ou ativos digitais ainda não está definida no marco regulatório brasileiro. Esse vácuo normativo foi identificado pela equipe de compliance da Neoenergia como o principal bloqueador para produção, não a tecnologia em si. A recomendação para projetos similares: engajar o time jurídico desde a fase de arquitetura, não após o desenvolvimento da PoC.

6. Conclusão e Trabalhos Futuros

Este estudo de caso documenta a colaboração entre CPQD e Neoenergia na construção de uma infraestrutura de cibersegurança para o mercado de I-RECs, demonstrando que é possível eliminar as vulnerabilidades críticas do modelo manual (double retirement, ausência de não-repúdio, falta de atomicidade) com throughput e custo compatíveis com operação industrial.

As três propriedades de segurança centrais, unicidade criptográfica via ERC-721, aposentadoria irreversível com prova on-chain e DvP atômico, foram validadas em mais de 18.000 transações, com taxa de falha de 0,27% e custo de ciclo de vida abaixo de US$ 0,08 por certificado.

Para trabalhos futuros, prevemos: (i) implementação de Provas de Conhecimento Zero (ZKP) para validar volumes de geração sem expor dados operacionais sensíveis; (ii) integração nativa com a API Evident para automação completa do ciclo de emissão; (iii) avaliação de redes L2 para redução de custo e variabilidade de gás em produção.

7. Agradecimentos

Os autores agradecem o apoio fornecido a este trabalho pela TERMOPERNAMBUCO S.A., empresa do Grupo Neoenergia, no âmbito do projeto de P&D PD-00290-0055/2024, financiado pelo Fundo de P&D da ANEEL. A execução foi realizada com a ativa participação do CPQD como Instituição Científica, Tecnológica e de Inovação (ICT).

Referências

CCEE (2023). Relatório de operações do mercado de energia elétrica, 2023. Technical report, Câmara de Comercialização de Energia Elétrica.

Evident (2022). Evident code for i-rec (electricity), version 1.1. `https://drive.google.com/file/d/1vwntAdB0EoQagzwOjTheoOI0ahstTWtU/view`.

Instituto Totum (2024). I-rec services. `https://site.institutototum.com.br/totum-services/i-rece/`.

Liu, W.-J., Chiu, W.-Y., and Hua, W. (2024). Blockchain-enabled renewable energy certificate trading: A secure and privacy-preserving approach. *Energy*, 290:130110.

Yamaguchi, J. A. R., Santos, T. R., and Carvalho, A. P. (2021). Blockchain technology in renewable energy certificates in brazil. *Brazilian Administration Review*, 18(Special Issue):e200069.