Análise e melhoria da segurança de aplicação do padrão T-REX na emissão de tokens fungíveis e não fungíveis para certificados de energia renovável

José Roberto Vieira Junior, Marco Amaral Henriques

Faculdade de Engenharia Elétrica e de Computação
Universidade Estadual de Campinas
Campinas – São Paulo – Brasil

vjr.joseroberto@gmail.com, maah@unicamp.br

Resumo. *A crescente demanda por energia renovável criou o mercado de Certificados Internacionais de Energia Renovável (I-REC), cuja comercialização tem baixa transparência e risco de fraudes. O comércio de I-RECs pode ser melhor controlado com emissão de tokens fungíveis e não fungíveis (ERC-1155). Mas, para serem considerados ativos do mundo real, precisam seguir leis financeiras e a combinação com o protocolo ERC-3643, Token for Regulated EXchanges (T-REX), permite tal regulação on-chain. Este trabalho em andamento avalia a segurança de uma implementação T-REX com ERC-1155 e descreve vulnerabilidades, que podem ser corrigidas com custo de gas inferior a 25.000 nas operações recorrentes e a 655.000 na instalação inicial.*

Abstract. *The growing demand for renewable energy has created the market for International Renewable Energy Certificates (I-RECs), whose commercialization suffers from low transparency and fraud risks. The trading of I-RECs can be better controlled through the issuance of fungible and non-fungible tokens (ERC-1155). However, to be considered real-world assets, they must comply with financial laws, and the combination with the ERC-3643 protocol, Token for Regulated EXchanges (T-REX), enables on-chain regulation. This work in progress assesses the security of a T-REX implementation using ERC-1155 and describes vulnerabilities that can be mitigated at a gas cost below 25,000 for recurring operations and 655,000 for the initial deployment.*

1. Introdução

A rede elétrica é fortemente interconectada e construir uma infraestrutura de transmissão e distribuição para cada consumidor é inviável economicamente. Logo, a energia que chega a qualquer ponto de consumo é uma mistura indistinta de toda a matriz de geração do sistema. Isso torna impossível para o consumidor rastrear diretamente a origem da eletricidade que consome. Esse problema se acentua com a crescente demanda por sustentabilidade. Para resolver isso, surgiram os Certificados de Energia Renovável

Os autores agradecem o apoio fornecido para este trabalho pelo Grupo Neoenergia e pela TERMOPERNAMBUCO S.A., no âmbito do Projeto de P&D Aneel PD-00290-0055/2024, financiado pelo Fundo de P&D da ANEEL. Este projeto foi realizado com a participação do CPQD. O trabalho contou com auxílio de ferramentas de IA na revisão do texto e na depuração de códigos.

(RECs), instrumentos contábeis e legais que atribuem o consumo de uma unidades de energia (1 MWh, por exemplo) à entidade que os adquire.

Durante anos, padrões regionais distintos dificultaram a interoperabilidade desse mercado. O padrão I-REC (*International Renewable Energy Certificate*) unificou o mercado em uma solução global [1]. No Brasil, onde cerca de 88,2% da matriz energética já é renovável, o I-REC tem papel central para consolidar o país como referência em ativos ambientais [6]. O contraste, porém, é gritante: o país gera anualmente o equivalente a 672 TWh de eletricidade renovável, mas em 2023 apenas 6,9% disso foi representado por certificados. Projeções sugerem que esse percentual pode chegar a 50% à medida que a rastreabilidade melhore e os riscos de dupla contagem sejam reduzidos.

A tecnologia *blockchain* e a evolução da rede Ethereum [2] trouxeram infraestruturas capazes de automatizar a validação desses ativos via tokens e contratos inteligentes de acordo com padrões ERC (*Ethereum Request for Comments*). Mas migrar para *marketplaces* experimentais exige mais que automação: exige conformidade. É nesse ponto que o protocolo ERC-3643 (T-REX *Token for Regulated EXchanges* [3]) se diferencia de outros, como ERC-20, ERC-721 e ERC-1155, focados na geração de tokens e sua fungibilidade [4] (intercambialidade entre unidades de um mesmo ativo). Com camadas de identidade descentralizada e governança *on-chain*, o protocolo já chamou atenção do Banco de Compensações Internacionais (BIS) por permitir tratar o I-REC como um Ativo do Mundo Real Tokenizado (RWA) em conformidade com reguladores como a CVM (Comissão de Valores Mobiliários) [5]. O potencial regulatório do ERC-3643, porém, esbarra em problemas práticos de protocolos que exigem múltiplas validações de conformidade. Este trabalho avalia a segurança e propõe melhorias em uma implementação do protocolo T-REX sobre tokens fungíveis e não fungíveis do padrão ERC-1155 [7].

O artigo está organizado como segue: A Seção 2 apresenta os fundamentos de RECs e sua tokenização em *blockchain* com ERC-1155 e ERC-3643. A Seção 3 discute a conformidade regulatória dos padrões. A Seção 4 detalha a metodologia de análise. A Seção 5 apresenta as vulnerabilidades identificadas e mitigações e a Seção 6 descreve as conclusões e possíveis trabalhos futuros.

2. Certificados de Energia Renovável I-REC e seus *tokens* em *blockchain*

2.1. Certificados I-REC

O *I-REC Standard* surgiu para unificar o mercado em uma solução internacional e globalmente aceita, garantindo credibilidade e auditabilidade dos certificados em diferentes jurisdições. No modelo tradicional, a integridade e a exclusividade do I-REC dependem de um registro centralizado. A emissão do certificado passa pela validação de metadados de produção feita por entidades certificadoras no Brasil.

O fluxo é essencialmente *off-chain*: os dados são enviados para entidades acreditadas, que os auditam manualmente ou de forma semiautomática e registram o certificado num banco de dados centralizado. O modelo funciona, mas com limitações que ficam evidentes conforme a demanda cresce, mostrando problemas como latência, vulnerabilidade sistêmica e assimetria de informação.

2.2. Evolução dos padrões de tokenização

Os padrões ERC definem as regras técnicas e a interoperabilidade para criação de ativos digitais. Trabalhos recentes como Haryani et al. [15] já adotam o ERC-1155 para tokenização de RECs no contexto indonésio, demonstrando que o padrão é uma escolha estabelecida na literatura para certificados semifungíveis. O diferencial deste trabalho está na adição da camada de conformidade regulatória digital e na análise sistemática de segurança resultante dessa combinação.

O ERC-20 não provê identidade única ao token, o ERC-721 não permite fracionamento de tokens e o ERC-1155 é híbrido, permitindo ambos. Nenhum deles, porém, resolve a conformidade institucional com regras que regem o sistema financeiro. O ERC-3643 (T-REX) acrescenta uma camada de gestão de identidade sobre os tokens, restringindo as transações a carteiras verificadas e habilitando funções como congelamento ou recuperação de ativos por ordem judicial ou regulatória. É essa camada que viabiliza a integração com bolsas de valores e outros ambientes regulados, pois traz recursos como *Know Your Customer* (KYC) e *Anti-Money Laundering* (AML).

2.3. Estrutura de dados e conformidade *on-chain*

O ERC-1155 cuida da rastreabilidade técnica via metadados, mas o ERC-3643 vai além: torna a identidade um requisito de validação *on-chain*. Essa governança é sustentada por quatro contratos inteligentes interdependentes: *Registro de identidade*, *Armazenamento de registro de identidade*, *Conformidade (Compliance)* e *Registro de emissores confiáveis*. Juntos, esses contratos viabilizam a verificação dinâmica de credenciais via ONCHAINID[1], garantindo que só agentes em conformidade com restrições regionais e regulatórias consigam transacionar. A imutabilidade do processo impede que um mesmo certificado seja vendido para múltiplos compradores e permite que o emissor mantenha controle de conformidade, o que torna o modelo viável para a gestão de RWA tokenizados.

3. Conformidade regulatória dos padrões de tokenização

A transição do I-REC para o ambiente *on-chain* não é uma simples troca de plataforma: é uma reengenharia da infraestrutura de confiança, onde a imutabilidade algorítmica e a atestação criptográfica substituem a verificação centralizada. Esta seção compara os modelos tradicionais com aqueles baseados em ERC-3643, considerando eficiência operacional e aderência regulatória. No mundo financeiro real é preciso que os contratos inteligentes atendam regras de *compliance* dos custodiantes locais e é justamente aí que os padrões divergem de forma significativa. A Tabela 1 detalha essa comparação frente às exigências para negociação de ativos financeiros regulados.

Os padrões ERC-20, ERC-721 e ERC-1155 não oferecem mecanismos de controle digital para o mercado financeiro. O ERC-3643 preenche essa lacuna ao integrar nativamente *ONCHAIND*, permitindo liquidez atômica da *blockchain* dentro de regras de conformidade institucional. A escolha do ERC-1155 como padrão-base justifica-se pela sua natureza híbrida (fungível e não fungível) e pela capacidade de gerenciar múltiplos ativos sob um mesmo contrato. Alternativas como ERC-1400, que possui modelo de *compliance* somente para *tokens* fungíveis, e ERC-3525, que introduz subcontas desnecessárias, são menos flexíveis e eficazes para os propósitos em questão.

[1]Padrão de identidade descentralizada dentro da *blockchain* para verificação de credenciais.

Tabela 1. Análise de Conformidade: requisitos CVM vs. padrões de tokenização

Característica	**CVM**	**ERC-20**	**ERC-721**	**ERC-1155**	**ERC-3643**
Tipos de Investidor	OK	X	X	X	OK
Origem dos Dados	OK	X	X	X	OK
Monitoramento	OK	OK	OK	OK	OK
Movimentação	OK	X	X	X	OK
Escrituração	OK	OK	OK	OK	OK
Liquidação	D+2	Atômica			
Dividendos	OK	OK (Airdrop)			OK
Governança	OK	X	X	X	OK
Votos	OK	X	X	X	OK
Auditorias	periódicas	via blockchain			
Pausa (Judiciário)	OK	X	X	X	OK
Recuperação	OK	X	X	X	OK
Limitação de ID	OK	X	X	X	OK
Queima/Liquidação	OK	OK	OK	OK	OK
Emissão/Resgate (Mint/Call)	OK	OK	–	OK	OK

A *blockchain* elimina o risco de dupla contagem e o ERC-1155 provê rastreabilidade com frações fungíveis de energia, mas a conformidade regulatória exige mais que isso. Automatizá-la reduz o erro humano, mas desloca o vetor de ataque do usuário individual para as entidades certificadoras. Um ataque bem-sucedido a elas é mais difícil, mas pode comprometer milhares de identidades de uma vez, abrindo caminho para que agentes maliciosos operem como aprovados.

4. Metodologia

Pelas discussões anteriores fica clara a importância do padrão ERC-1155 para a emissão de tokens fungíveis e não fungíveis ligados a ativos ambientais e a dificuldade de tornar esses tokens seguros o bastante para serem aceitos como ativos no mundo real. Portanto, existe um desafio na aplicação das ideias do padrão de segurança de tokens ERC-3643 (T-REX) aos tokens de energia renovável IREC emitidos segundo a ERC-1155, tornando mais seguras e confiáveis as transações envolvendo tais tokens.

O protocolo T-REX oficial [3] não oferece suporte nativo ao padrão ERC-1155. Uma implementação da comunidade [7] estende o T-REX sobre ERC-1155 usando o padrão Diamond EIP-2535 e, até onde foi possível apurar, é a única a combinar T-REX com *tokens* fungíveis e não fungíveis. Entretanto, não há, nesse trabalho ou na literatura, uma análise sistemática de segurança desse protocolo sob a ótica de transferência de *tokens*, governança de *facets* e controle de acesso em ambiente multi-ativo. O código com as correções propostas está disponível em [8]. Nesse contexto, este trabalho se propõe a identificar, demonstrar e mitigar as vulnerabilidades presentes nessa implementação do T-REX sobre os mecanismos de emissão de tokens.

Esta fase inicial foi estruturada em cinco etapas: (i) revisão da literatura sobre vulnerabilidades em contratos inteligentes, cobrindo reentrância [11], controle de acesso e proxies atualizáveis [14]; (ii) análise arquitetural da implementação Diamond do ERC-

3643 com ERC-1155; (iii) exame do código-fonte focado em transferência de tokens, atualização de *facets* e RBAC; (iv) exploração de cada vulnerabilidade via PoC em Solidity com Foundry [9] na rede Anvil; e (v) mitigação validada por testes automatizados com medição de *gas*[2] via `forge snapshot`. As três vulnerabilidades encontradas decorrem da arquitetura do protocolo — *callback* obrigatório do ERC-1155, `diamondCut` sem proteção temporal e RBAC global. Portanto são intrínsecas à combinação do T-REX com ERC-1155 sobre Diamond.

5. Vulnerabilidades identificadas e resultados

5.1. Vulnerabilidade 1 — Reentrância no ERC-1155

O método `ERC1155Facet` implementa `safeTransferFrom` em conformidade com o ERC-1155, que exige a invocação do callback `onERC1155Received` no contrato de quem recebe após a atualização de saldo. O *callback* é uma superfície de ataque conhecida , mas não aparece no código analisado, permitindo reentrância [14].

A PoC implementa um contrato `DrainingReceiver` que, ao receber esse *callback*, invoca novamente o `safeTransferFrom` em nome da vítima aprovada previamente no `setApprovalForAll`. O resultado final é: a vítima inicia com N unidades de token, tem uma transferência autorizada de M unidades e, após o ataque, ela acaba com saldo zerado. Os $N - M$ tokens de diferença são enviados para o endereço do atacante que os recebe sem autorização. O experimento foi executado em rede local Anvil e confirmado por script *Forge*. Esse padrão é análogo ao vetor explorado no ataque ao The DAO em 2016 e a incidentes posteriores.

Para esse vetor de ataque deixar de existir, foi utilizada a biblioteca OpenZeppelin ReentrancyGuard [12]. Essa abordagem é a recomendada pelo OWASP SCWE-138 [14] e pelo ConsenSys Best Practices [13]. Foi preciso assumir um custo extra em *gas*, com um *overhead* de +23.872 por chamada (um acréscimo de 16,6% sobre o original). Este custo adicional é razoável diante do risco de se perder todo o saldo disponível.

5.2. Vulnerabilidade 2 — Ausência de Timelock no `diamondCut`

O padrão de proxy Diamond (ERC-2535) centraliza a atuação do protocolo na função `diamondCut`, que tem a sua proteção de acesso feita pelo desenvolvedor [10]. A ausência de uma trava temporal Timelock é crítica: esse problema é conhecido desde 2020 e formalizado pelo OWASP como SCWE-005 [14]. Na implementação do T-REX sobre o proxy Diamond não há a implementação desse mecanismo de controle de tempo.

A PoC demonstrou que, se a chave do *owner* é comprometida ou se há atuação de um *owner* malicioso, é possível substituir qualquer *facet* do protocolo em uma única transação. Foi criado um contrato `MaliciousERC1155Facet`, executando transferências sem qualquer aviso prévio aos detentores. Esse vetor é classificado pelo OWASP como SC10:2026 e está entre as dez vulnerabilidades mais críticas do ecossistema. Para mitigar esse vetor, foram introduzidos *timelocks* em três funções e no *owner*, validados por testes que comprovam: (i) o ataque é possível sem *timelocks*; (ii) com *timelocks* ativos a chamada reverte; (iii) o fluxo *propose* + *wait* + *execute* funciona corretamente e impede a re-execução. Qualquer proposta de *upgrade* deve aguardar o período de *timelock* antes

[2]Unidade de custo computacional da EVM (Ethereum Virtual Machine).

da execução, impedindo alterações maliciosas instantâneas. Essas novas implementações têm custo único de *gas* de 654.942 na instalação (*deploy*) do contrato.

5.3. Vulnerabilidade 3 — RBAC Global Excessivamente Permissivo

O `SupplyFacet` original verifica a autorização de *mint* e *burn* por meio de um papel global (`ISSUER_ROLE`) sem restrição ao tokenId operado. Esse padrão configura uma violação do princípio do menor privilégio documentada pela literatura como *over-privileged role*, a qual é considerada vulnerabilidade de controle de acesso de alta criticidade [14]. Em um protocolo ERC-1155 os certificados de diferentes usinas seriam insuficientes para uma escalada de privilégios e um emissor do ativo A poderia emitir B.

Para a PoC foi criado o contrato `test_GlobalRoles_OverPermissive` que demonstrou que, após receber `ISSUER_ROLE` global, um operador realiza uma emissão (*mint*) bem-sucedida tanto no *tokenId* 1 quanto no *tokenId* 2, resultando em X e Y unidades para o destinatário. Para esse vetor de ataque deixar de existir, foram implementados os papéis *token-scoped* por meio de dois componentes: (i) extensão do *storage* com o mapeamento das regras do *token slot* previamente não utilizado; (ii) substituição do *SupplyFacet* pelo *SupplyFacetMigrated* com verificação global do *tokenId*. A PoC confirmou que, após as alterações, o operador não pôde fazer a emissão como antes. O custo em *gas* para isso foi de +173 ou (+0,1%), desprezível em termos práticos. A Tabela 2 resume as três vulnerabilidades identificadas, com as mitigações e o custo de *gas* associado.

Tabela 2. Síntese das vulnerabilidades identificadas e mitigações propostas

Vulnerabilidade	Mitigação	*Gas*
Reentrância ERC-1155	`nonReentrant`	$+23.872$ por transação
DiamondCut sem timelock	Timelock propose+execute	$+654.942$ (só *deploy*)
RBAC global permissivo	Token-scoped roles	$+173$ por transação

6. Conclusões

Este trabalho focou na necessidade de se aplicar controles mais rigorosos a sistemas de comercialização de tokens relacionados a ativos ambientais, mais especificamente aqueles ligados ao International Renewable Energy Certificate (I-REC), para que estes possam ser tratados como ativos válidos e negociáveis no mundo real. Nesse contexto, o trabalho avaliou uma implementação pública do protocolo ERC-3643 (T-REX) sobre o padrão Diamond EIP-2535 com suporte a tokens ERC-1155 e identificou três tipos de vulnerabilidade de segurança nessa implementação: reentrância via *callback* obrigatório do ERC-1155, ausência de *timelock* em `diamondCut` e RBAC excessivamente permissivo em ambiente multi-ativo. A principal contribuição é a análise sistemática de segurança da camada de conformidade regulatória *on-chain*. O custo agregado de duas das três correções nas operações recorrentes do protocolo é inferior a 25000 *gas* por transação, valor aceitável diante do risco mitigado. O maior custo é de 655000 no *timelock*, mas ele ocorre uma única vez no *deploy* do contrato. Como trabalhos futuros, propomos: (i) comparar o ERC-1155 com ERC-1400 e ERC-3525 quanto à segregação de classes de ativo; (ii) avaliar a escalabilidade do *timelock* em soluções L2; (iii) investigar *timelocks* parametrizáveis por *facet* com mecanismos de revogação de emergência e (iv) investigar a integração do T-REX com moedas digitais de banco central (CBDC), como o DREX brasileiro, aplicando a camada de conformidade regulatória *on-chain* à liquidação de ativos ambientais tokenizados em sistemas de liquidez digital [5].

Referências

[1] International Energy Agency, "Product Code for Electricity: The International Attribute Tracking Standard version 1.1," . Available: https://www.trackingstandard.org/.

[2] V. Buterin et al., "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2013. Available: https://ethereum.org/en/whitepaper/

[3] J. Lebrun et al., "ERC3643: The T-REX protocol (Token for Regulated Exchanges) - Version 4.0," Tokeny Solutions, Mar. 2023. . Available: https://github.com/ERC-3643/ERC-3643.

[4] W. Radomski, A. Cooke, P. Castonguay, J. Therien, E. Binet, and R. Sandford, "ERC-1155: Multi Token Standard," Ethereum Improvement Proposals, no. 1155, Jun. 2018. . Available: https://eips.ethereum.org/EIPS/eip-1155.

[5] M. Aquilina, U. Lewrick, F. Ravenna, and L. Schönleber, "The rise of tokenised money market funds," BIS Bulletin, no. 115, Bank for International Settlements, Nov. 2025.

[6] Empresa de Pesquisa Energética (EPE), "Summary Report of the Brazilian Energy Balance 2025 — base year 2024." Available: https://www.epe.gov.br/en/publications/publications/brazilian-energy-balance-2025.

[7] R. Correia, "diamond-erc3643-protocol," Available: https://github.com/renancorreadev/diamond-erc3643-protocol.

[8] J. R. Vieira Junior, "diamond-erc3643-hardening fork do https://github.com/renancorreadev/diamond-erc3643-protocol," Available: https://github.com/vjr-joseroberto/diamond-erc3643-hardening.

[9] Paradigm, "Foundry: Ethereum development toolkit," Available: https://github.com/foundry-rs/foundry.

[10] Ethereum Foundation, "EIP-2535: Diamonds, Multi-Facet Proxy," Available: https://eips.ethereum.org/EIPS/eip-2535.

[11] M. Mehar, C. Shier, A. Giambattista, E. Gong, G. Fletcher, R. Sanayhie, H. M. Kim, and M. Laskowski, "Understanding a Revolutionary and Flawed Grand Experiment in Blockchain: The DAO Attack," Journal of Cases on Information Technology, vol. 21, no. 1, pp. 19–32, 2019. DOI: 10.4018/JCIT.2019010102.

[12] OpenZeppelin, "Security API - ReentrancyGuard," Available: https://docs.openzeppelin.com/contracts/4.x/api/security.

[13] Consensys, "Solidity Best Practices for Smart Contract Security," Available: https://consensys.io/blog/solidity-best-practices-for-smart-contract-security.

[14] OWASP Foundation, OWASP Smart Contract Security Available: https://scs.owasp.org/.

[15] P. Haryani et al., "Blockchain-based renewable energy certificate management system using semi-fungible token," Heliyon, vol. 11, e42364, 2025. DOI: 10.1016/j.heliyon.2025.e42364.