Implementação e Benchmarks de uma Arquitetura Factory-Beacon-ERC-1155 para Tokenização Multi-Ativo de Commodities Agrícolas

Juan Minango[1], **Alberto Paradisi**[1], **Silvia Marion**[1], **Andreza Lona**[1]

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

{b_64408, paradisi, marion, andreza}@cpqd.com.br

Abstract. *Deploying individual smart contracts per agricultural asset class is cost-prohibitive, and immutable ERC-20/ERC-721 contracts require full redeployment for every protocol update. We propose and implement a unified architecture combining Factory with CREATE2 deterministic addressing, Beacon Proxy upgradeability, and ERC-1155 multi-token capabilities. Evaluated via Foundry gas benchmarks, the architecture reduces batch minting cost by 38% and keeps protocol-wide upgrades at a constant 5,439 gas regardless of proxy count, compared to 280,863 gas per contract for traditional redeployment.*

Resumo. *A implantação de contratos individuais por classe de ativo agrícola é economicamente inviável em escala, e contratos ERC-20/ERC-721 imutáveis exigem redeploy completo a cada atualização. Propomos e implementamos uma arquitetura que integra Factory com endereçamento determinístico CREATE2, Beacon Proxy e ERC-1155. Avaliada via benchmarks de gas no Foundry, a arquitetura reduz a emissão em lote em 38% e mantém atualizações de protocolo em 5.439 gas por transação, independentemente do número de proxies, contra 280.863 gas por contrato na abordagem convencional.*

1. Introdução

O acesso ao crédito rural é um dos principais gargalos para a agricultura familiar no Brasil. Segundo [Climate Policy Initiative 2023], apenas 15% dos agricultores familiares obtêm crédito rural formal, apesar de representarem cerca de 75% dos estabelecimentos rurais, com acesso ainda mais restrito para os menores produtores. A tecnologia blockchain surge como alternativa para desburocratizar esse acesso por meio da tokenização de Ativos do Mundo Real (RWA), permitindo o investimento direto na produção agrícola [World Economic Forum 2025].

Na prática, implantar cada ativo tokenizado como um contrato inteligente (*smart contract*) independente apresenta custos proibitivos em cenários com múltiplos ativos [Salehi et al. 2022, Bodell et al. 2023]. A fragmentação entre os padrões ERC-20 (commodities fungíveis, como café e mel) e ERC-721 (ativos únicos, como gado) força implantações separadas [Radomski et al. 2018], e uma vez implantados, contratos são imutáveis por natureza, exigindo migração completa a cada atualização necessária [Salehi et al. 2022]. A imprevisibilidade dos endereços no momento de implantação complica ainda mais a integração com sistemas legados de gestão agrícola.

A abordagem adotada combina Factory, Beacon Proxy [Bodell et al. 2023] e CREATE2 [Buterin 2018] sobre o ERC-1155 [Radomski et al. 2018], formando uma arquitetura modular para tokenização multi-ativo. A implementação completa foi desenvolvida em Solidity e avaliada por meio de benchmarks de gas com o framework Foundry, gerando evidências quantitativas comparativas com a abordagem ERC-20/ERC-721 convencional, com destaque para a redução de 99,4% no custo de atualização do protocolo.

A literatura em blockchain agrícola concentra-se principalmente em rastreabilidade na cadeia de suprimentos [United Nations Development Programme 2021], com foco em transparência e verificação de procedência para café, gado, grãos e horticultura. Trabalhos recentes sobre tokenização de ativos do mundo real [Xia et al. 2025, Muzondo et al. 2025] ainda adotam ERC-20 ou ERC-721 de forma separada, forçando implantações distintas por classe de ativo e sem resolver atualizações de protocolo. Mecanismos de upgrade via proxy foram estudados de forma isolada [Salehi et al. 2022], porém sem combinação com endereçamento determinístico ou suporte multi-ativo. A Tabela 1 sintetiza essas dimensões; a combinação das quatro propriedades com validação experimental ainda não foi identificada na literatura revisada.

Tabela 1. Posicionamento em relação à literatura.

Trabalho	Multi-token	Atualizável	Det. addr.	Exp.
[United Nations Development Programme 2021]	–	–	–	sim
[Xia et al. 2025]	–	–	–	parcial[1]
[Salehi et al. 2022]	–	sim	sim	–
[Muzondo et al. 2025]	–	–	–	–
[Olateju 2025]	–	–	–	–
Este trabalho	**sim**	**sim**	**sim**	**sim**

Do ponto de vista de sistemas distribuídos, o Beacon garante coerência do protocolo por construção, pois todos os proxies referenciam dinamicamente a mesma lógica vigente sem comunicação direta entre si. O CREATE2 viabiliza integração pré-existência (*pre-deployment integration*) com sistemas legados, sem necessidade de sincronização pós-deploy.

2. Arquitetura Proposta

A arquitetura é composta por quatro componentes com papéis complementares, descritos a seguir.

Contrato de implementação (AgroTokenV1). Herda do ERC-1155 e fornece interface unificada para ativos fungíveis (`amount` > 1) e não-fungíveis (`amount` $= 1$), eliminando contratos ERC-20 e ERC-721 separados. Não mantém estado próprio; toda execução ocorre no contexto de armazenamento do proxy via `delegatecall`.

Beacon. Armazena o endereço da implementação vigente, consultado por todos os proxies a cada chamada. Cada instância de **BeaconProxy** mantém armazenamento isolado de uma categoria de ativo e delega a execução ao Beacon, permitindo que uma única transação de atualização propague nova lógica para toda a frota instantaneamente.

[1] Análise conceitual com estimativas de custo, sem deploy em testnet ou medições diretas de gas.

Factory (AgroFactory). Calcula o *salt* como `keccak256(abi.encode(assetType, region, year, producer))`, garantindo endereçamento determinístico, e implanta BeaconProxy via CREATE2. Mantém registro enumerável de todos os proxies criados.

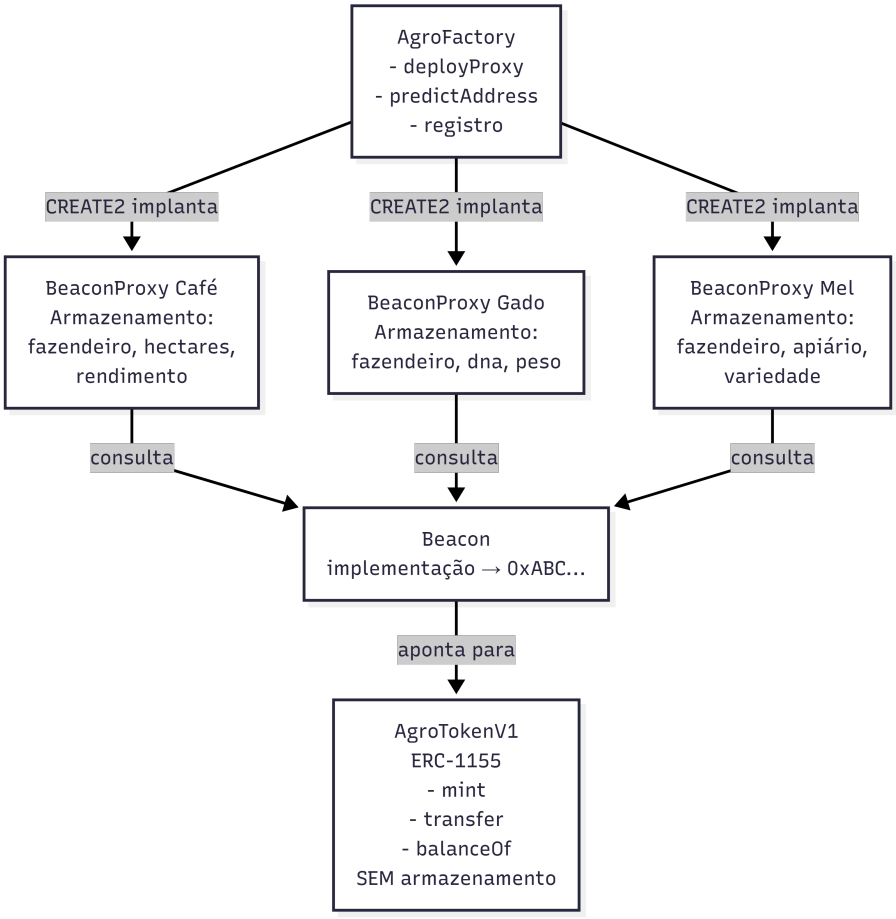

Figura 1. `AgroFactory` implanta proxies via CREATE2 (1); cada `BeaconProxy` redireciona chamadas via `delegatecall` ao `Beacon` (2), que retorna o endereço vigente do `AgroTokenV1` para execução no contexto do proxy (3). Uma chamada `upgradeImplementation` propaga nova lógica para toda a frota.

3. Implementação

Os contratos foram implementados em Solidity 0.8.28, utilizando a biblioteca OpenZeppelin v5.6.1. O código-fonte, incluindo os testes e os benchmarks de gas, está disponível em: `https://github.com/jminango20/agro-tokenization`.

AgroTokenV1.sol herda de `ERC1155Upgradeable` e `AccessControlUpgradeable`. A estrutura `TokenMetadata` armazena *on-chain* os atributos do ativo (tipo, região, ano, produtor e indicador de fungibilidade). A operação `mint` recebe esses metadados junto com o destinatário, ID e quantidade; `mintBatch` permite emissão de múltiplos tipos em uma única transação.

AgroFactory.sol herda de `Ownable` e possui referência imutável ao Beacon (do qual é proprietário, habilitando a função `upgradeImplementation`). A implantação

determinística combina o bytecode de `BeaconProxy` com os dados de inicialização para gerar o endereço antes do deploy, via `Create2.computeAddress`. Isso permite que sistemas de gestão agrícola legados registrem o endereço do contrato antes da sua existência na rede.

Os três casos de uso abrangidos, resumidos na Tabela 2, são instanciados como proxies independentes por meio da Factory.

Tabela 2. Casos de uso implementados e suas características de token.

Proxy	Tipo de token	amount	Exemplo de ID
Café	Fungível	> 1	Lote por safra/região
Gado	Não-fungível	$= 1$	Animal individual
Mel	Híbrido (ambos)	$= 1$ / > 1	Colônia / Lote de mel

O caso do mel demonstra bem a flexibilidade do ERC-1155. Por convenção de implementação, IDs < 1000 representam colônias (NFT, `amount` = 1) e IDs ≥ 1000 representam lotes de mel (fungível, `amount` > 1), tudo dentro de um único contrato proxy, sem nenhuma mudança de lógica.

Análise de Segurança. O modelo de adversário considera um atacante capaz de submeter transações arbitrárias, sem quebrar primitivas criptográficas. Três vetores são endereçados: (1) comprometimento da chave de upgrade, mitigado com multisig e timelock; (2) emissão não autorizada, bloqueada pelo `MINTER_ROLE` via `AccessControlUpgradeable`; (3) colisão de endereço CREATE2, inviável pela resistência à pré-imagem do keccak256. A separação de armazenamento via *unstructured storage* (EIP-1967 [Palladino et al. 2019]) previne colisões de slot; reentrância em callbacks `onERC1155Received` é mitigada pelo padrão *checks-effects-interactions* do OpenZeppelin [Bodell et al. 2023].

4. Avaliação Experimental

Os experimentos foram conduzidos com Foundry v1.5.1-stable sobre EVM *cancun* via `forge test --gas-report`. O custo de gas é determinístico por definição da especificação EVM [Wood 2024]: bytecode e estado de entrada idênticos produzem exatamente o mesmo consumo em qualquer execução, tornando medições únicas plenamente reprodutíveis sem necessidade de tratamento estatístico. A infraestrutura completa (Factory + Beacon + Implementação) custa 4.812.982 gas, cobrado *uma única vez*. Cada BeaconProxy adicional exige 360.831 gas, contra 280.863 (ERC-20) ou 322.549 (ERC-721) para contratos tradicionais. A Tabela 3 detalha as demais operações.

O custo individual de *mint* é superior na arquitetura proposta porque cada chamada atravessa dois saltos adicionais de `delegatecall` (Proxy $\rightarrow$ Beacon $\rightarrow$ Implementação), overhead de aproximadamente 74 kgas em relação ao ERC-20 direto. Esse resultado deve ser interpretado no contexto do fluxo real de emissão agrícola. Cooperativas e produtores tokenizam lotes completos de café ou mel ao final de cada ciclo produtivo, e bovinos são registrados em grupos no momento de eventos de manejo (vacinação, pesagem). A operação unitária raramente ocorre de forma isolada. Quando avaliada no padrão de uso predominante, a emissão em lote, a arquitetura é 38,0% mais

Tabela 3. Custo de gas (unidades): arquitetura proposta vs. tradicional.

Operação	Proposta	Tradicional	Variação
Deploy por ativo	360.831	280.863 (ERC-20)	+28,5%
		322.549 (ERC-721)	+11,8%
Mint fungível	129.438	55.032 (ERC-20)	+135%
Mint NFT	129.438	77.090 (ERC-721)	+67,9%
Batch mint (3 tipos)	87.174	141.164 (3×ERC-20)	−38,0%
Atualização (N proxies)	**5.439**	**842.325** (3 redeployments)	**−99,4%**

econômica. O `mintBatch` de 3 tipos custa 87.174 gas contra 141.164 gas para 3 contratos distintos chamados individualmente.

A vantagem mais expressiva reside na atualização. Enquanto a abordagem convencional exige o redeploy de cada contrato (842.325 gas para 3 contratos), uma única chamada `upgradeImplementation` à Factory consome apenas 5.439 gas e atualiza *toda* a frota de proxies simultaneamente. Para N proxies, o custo de atualização permanece constante em $O(1)$, enquanto o custo tradicional cresce linearmente em $O(N)$. A Figura 2 ilustra os dois argumentos centrais.

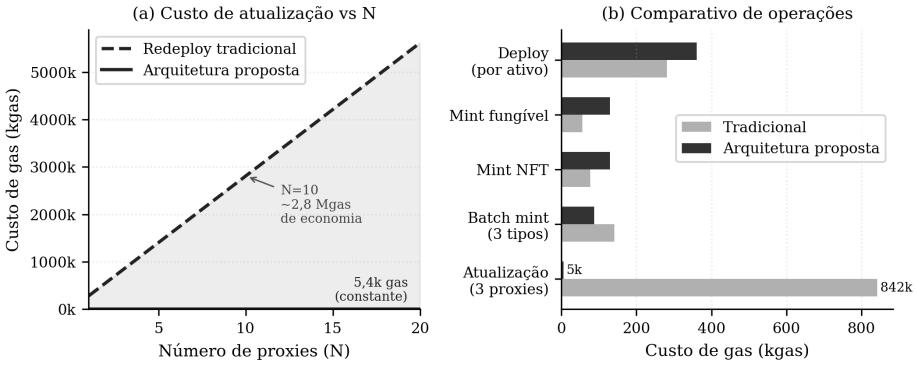

Figura 2. (a) Custo de atualização $O(1)$ via Beacon vs. $O(N)$ via redeploy. (b) Comparativo de gas por operação; barras escuras representam a arquitetura proposta.

5. Conclusão

A arquitetura Factory-Beacon-ERC-1155 se mostrou viável para tokenização de múltiplas commodities agrícolas. Os benchmarks confirmam 5.439 gas em $O(1)$ para atualizações e redução de 38% na emissão em lote; o overhead de `delegatecall` penaliza operações individuais de mint, tornando a solução mais adequada para plataformas com múltiplos ativos e atualizações periódicas.

As principais limitações são a concentração de controle no Beacon — mitigável com multisig e timelocks de 48–72 horas — e o crescimento de armazenamento *on-chain* proporcional a $O(N \times M)$ proxies e tokens, cujo custo acumulado deve ser considerado

em escala. A personalização por cooperativa é suportada via `AccessControl` (papéis por proxy) e extensão de `TokenMetadata` em novas versões de implementação. Estudos de caso com cooperativas agrícolas constituem o próximo passo.

Agradecimentos

Os autores agradecem o apoio da FAPESP (Processos 22/09319-9 e 24/18399-1) e do CPQD, Campinas, SP, Brasil.

Referências

Bodell, W. E., Meisami, S., and Duan, Y. (2023). Proxy hunting: Understanding and characterizing proxy-based upgradeable smart contracts in blockchains. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1829–1846, Anaheim, CA. USENIX Association.

Buterin, V. (2018). EIP-1014: Skinny CREATE2. Ethereum Improvement Proposals, no. 1014. Final. `https://eips.ethereum.org/EIPS/eip-1014`.

Climate Policy Initiative (2023). Agricultura familiar brasileira: Desigualdades no acesso ao crédito. Relatório, Climate Policy Initiative / PUC-Rio, Rio de Janeiro, Brasil.

Muzondo, P. J., Tapera, J., and Mashapure, R. (2025). The blockchain and tokenization for social good: Empowering smallholder farmers in zimbabwe's agricultural supply chains. *Dibon Journal of Education*. Acessado em novembro de 2025.

Olateju, O. (2025). Tokenization of agricultural assets: Strengthening blockchain security in agri-finance and investment models against fraud and cyber risks. SSRN Electronic Journal. SSRN 5162642.

Palladino, S., Giordano, F., and Croubois, H. (2019). EIP-1967: Proxy storage slots. Ethereum Improvement Proposals, no. 1967. Final. `https://eips.ethereum.org/EIPS/eip-1967`.

Radomski, W., Cooke, A., Castonguay, P., Therien, J., Binet, E., and Sandford, R. (2018). ERC-1155: Multi token standard. Ethereum Improvement Proposals, no. 1155. Final. `https://eips.ethereum.org/EIPS/eip-1155`.

Salehi, M., Clark, J., and Mannan, M. (2022). Not so immutable: Upgradeability of smart contracts on ethereum. In *Financial Cryptography and Data Security. FC 2022 International Workshops: CoDecFin, DeFi, Voting, WTSC, Grenada, May 6, 2022, Revised Selected Papers*, pages 539–554, Berlin, Heidelberg. Springer-Verlag.

United Nations Development Programme (2021). Blockchain for agri-food traceability. Technical report, UNDP Global Centre for Technology, Innovation and Sustainable Development. Acessado em dezembro de 2025.

Wood, G. (2024). Ethereum: A secure decentralised generalised transaction ledger. Technical report, Ethereum Foundation. Berlin Version. `https://ethereum.github.io/yellowpaper/paper.pdf`.

World Economic Forum (2025). Asset tokenization in financial markets: The next generation of value exchange. Technical report, World Economic Forum.

Xia, N., Zhao, X., Yang, Y., Li, Y., and Li, Y. (2025). Exploration on real world assets and tokenization. arXiv:2503.01111. `https://arxiv.org/abs/2503.01111`.