

Liquidação Atômica para Split Payment Tributário: Uma Prova de Conceito com Contratos Inteligentes no Contexto da Reforma Tributária Brasileira (LC 214/2025)

Resumo: Este trabalho investiga a viabilidade técnica da utilização de contratos inteligentes para a execução do mecanismo de split payment tributário previsto na Lei Complementar nº 214/2025, que regulamenta o Imposto sobre Bens e Serviços (IBS) e a Contribuição sobre Bens e Serviços (CBS) instituídos pela Emenda Constitucional nº 132/2023. Para tal, foi desenvolvida uma prova de conceito (PoC) que modela a liquidação atômica de transações comerciais com distribuição federativa automática dos tributos entre União, estados e municípios. A PoC implementa duas das três modalidades de split payment previstas na lei — o padrão (Art. 32) e o simplificado (Art. 33) — utilizando contratos inteligentes com verificação criptográfica de assinatura digital de um oráculo fiscal que simula a autoridade fazendária. Os resultados de 13 testes unitários demonstram que a arquitetura proposta garante: atomicidade na liquidação (o pagamento ao vendedor e a retenção tributária são indivisíveis), integridade dos dados fiscais (qualquer adulteração nos valores tributários é rejeitada automaticamente), idempotência (cada nota fiscal é processada uma única vez), compensação de créditos tributários conforme previsto na lei, e rastreabilidade completa via eventos imutáveis. O custo computacional médio foi de 168.713 unidades de gas para o split padrão e 114.268 para o simplificado. O trabalho discute as implicações dessa arquitetura para a gestão pública, contextualiza o abandono da plataforma Hyperledger Besu pelo Banco Central do Brasil no projeto DREX em novembro de 2025, e argumenta que a lógica de liquidação atômica é independente da infraestrutura subjacente, podendo ser transposta para diferentes plataformas tecnológicas.

Palavras-chave: Split Payment; Reforma Tributária; Contratos Inteligentes; Blockchain; Gestão Pública; IBS; CBS.

1. Introdução

A reforma tributária do consumo no Brasil, consolidada pela Emenda Constitucional nº 132/2023 e regulamentada pela Lei Complementar nº 214, de 16 de janeiro de 2025, representa a mais profunda reestruturação do sistema tributário brasileiro em três décadas. Em seu núcleo, a reforma substitui cinco tributos — PIS, COFINS, IPI (federais), ICMS (estadual) e ISS (municipal) — por dois: a Contribuição sobre Bens e Serviços (CBS), de competência federal, e o Imposto sobre Bens e Serviços (IBS), de competência compartilhada entre estados e municípios, gerido pelo Comitê Gestor do IBS. A transição será gradual, com início dos testes em 2026 e conclusão prevista para 2033.

Um dos pilares operacionais dessa reforma é o mecanismo de split payment, previsto nos artigos 31 a 35 da LC 214/2025. Trata-se de um sistema no qual o valor do tributo é automaticamente segregado do montante pago pelo adquirente e direcionado aos cofres públicos no momento exato da liquidação financeira da transação, antes que o fornecedor receba o valor líquido. Conforme apontam análises do Ministério da Fazenda (Brasil, 2025), o split payment transforma o fato gerador e o recolhimento em eventos sincronizados, inaugurando o que especialistas denominam “era da arrecadação em tempo real”.

A relevância do mecanismo se dimensiona pelo problema que pretende enfrentar. Estimativas do Instituto Brasileiro de Planejamento e Tributação (IBPT) apontam que a sonegação fiscal no Brasil alcança cifras na ordem de R\$ 417 bilhões anuais (Agência Brasil, 2020). A Receita Federal do Brasil, em seu relatório sobre o gap tributário do IRPJ/CSLL referente ao período 2015-2019, estimou que a sonegação correspondeu a 19% da arrecadação potencial média, enquanto os débitos declarados e não pagos representaram 18,1% adicionais (RFB, 2023). O split payment ataca diretamente essa segunda modalidade — a inadimplência fiscal — ao eliminar o intervalo temporal entre a ocorrência do fato gerador e o recolhimento do tributo.

Contudo, a implementação do split payment em escala nacional enfrenta desafios tecnológicos substanciais. A LC 214/2025 exige a vinculação em tempo real entre o documento fiscal eletrônico, o meio de pagamento e o repasse de tributos (Art. 32), o que demanda integração entre os sistemas da Receita Federal, do Comitê Gestor do IBS, das instituições financeiras e dos arranjos de pagamento. A lei prevê três modalidades — split padrão ou “inteligente” (Art. 32), simplificado (Art. 33) e de contingência (§4º, Art. 32) — cada uma com diferentes requisitos de infraestrutura e complexidade operacional.

Nesse contexto, a tecnologia de contratos inteligentes e de registros distribuídos tem sido apontada na literatura acadêmica como potencial instrumento para a gestão fiscal. Dourado et al. (2023) propuseram modelos de aplicação de blockchain fiscal ao sistema tributário brasileiro. Kim (2022), na *UCLA Law Review*, analisou iniciativas de blockchain para administração tributária, enquanto Ainsworth e Shact (2016) propuseram o uso de tecnologia de registro distribuído para arrecadação de IVA na União Europeia. No campo das experiências governamentais, a Rede Blockchain Brasil (RBB), fruto de cooperação entre o TCU e o BNDES, representa uma infraestrutura pública voltada a aplicações de interesse do Estado (Freitas & Vaz, 2022).

Entretanto, a trajetória do projeto DREX (Real Digital) do Banco Central do Brasil introduz um contraponto relevante. Após quatro anos de testes em fases piloto 1 e 2, o BCB desativou em novembro de 2025 a plataforma baseada em Hyperledger Besu, considerando-a inadequada aos requisitos de privacidade e segurança do sistema financeiro nacional e financeiramente onerosa (Forbes Brasil, 2025). A fase 3 do projeto, prevista para 2026, adotará uma abordagem agnóstica quanto à tecnologia, priorizando requisitos de negócio antes da definição da infraestrutura (Valor Econômico, 2025). Este evento reforça a necessidade de que

soluções tecnológicas para o sistema financeiro e tributário brasileiro sejam concebidas de forma independente da plataforma subjacente.

Diante desse cenário, este trabalho se propõe a responder à seguinte pergunta: é tecnicamente viável utilizar contratos inteligentes para executar o mecanismo de split payment tributário previsto na LC 214/2025, garantindo atomicidade na liquidação, integridade dos dados fiscais e distribuição federativa automática dos tributos? Para respondê-la, foi desenvolvida uma prova de conceito que implementa as modalidades de split padrão e simplificado, submetida a uma bateria de 13 testes unitários que avaliam funcionalidade, segurança e desempenho. A POC é concebida como demonstração de uma lógica de liquidação atômica independente de infraestrutura, podendo ser transposta para plataformas blockchain, APIs com assinatura digital, ou quaisquer outras tecnologias que o Banco Central ou o Comitê Gestor do IBS venham a adotar.

O artigo está estruturado da seguinte forma: a seção 2 apresenta o referencial teórico sobre split payment, tecnologias de registro distribuído e blockchain na gestão pública; a seção 3 descreve a metodologia e a arquitetura da prova de conceito; a seção 4 apresenta os resultados dos testes; a seção 5 discute as implicações para a gestão pública e as limitações do estudo; e a seção 6 traz as considerações finais e sugestões para agenda de pesquisa futura.

2. Referencial Teórico

2.1 O Split Payment como Mecanismo de Arrecadação Tributária

O conceito de split payment na tributação sobre o consumo consiste na segregação automática do tributo no momento do pagamento, de modo que o valor correspondente ao imposto seja direcionado diretamente ao fisco, sem transitar pela conta do fornecedor. A Comissão Europeia (2017), em seu relatório “Analysis of the Impact of the Split Payment Mechanism as an Alternative VAT Collection Method”, analisou o mecanismo como alternativa para redução do gap de arrecadação do IVA nos Estados-membros da União Europeia. O relatório identificou que, embora o split payment possa aumentar custos de conformidade para as empresas, ele apresenta potencial significativo de redução da inadimplência fiscal e da fraude carrossel.

No âmbito europeu, Itália e Polônia implementaram modalidades de split payment para o IVA. A Itália adotou em 2015 o mecanismo para pagamentos realizados por entidades públicas, expandindo-o posteriormente para transações com empresas listadas na bolsa de valores. A Polônia implementou em 2018 o split payment voluntário, tornando-o obrigatório em 2019 para setores específicos,

conforme autorização da Comissão Europeia (Vertexinc, 2019). Ainsworth e Musaad (2017) propuseram um modelo de coleta de IVA em tempo real baseado em tecnologia de registro distribuído, argumentando que a combinação de split payment com blockchain eliminaria estruturalmente a possibilidade de fraude por inadimplência.

No contexto brasileiro, a LC 214/2025 estabelece três modalidades de split payment. O split padrão, previsto no Art. 32, constitui o núcleo do sistema. Nele, a instituição financeira ou operadora do meio de pagamento, ao identificar a transação, consulta em tempo real os sistemas da Receita Federal e do Comitê Gestor do IBS para determinar o valor exato dos tributos a segregar, considerando inclusive o cruzamento entre débitos e créditos tributários do contribuinte. O split simplificado, previsto no Art. 33, oferece uma alternativa para operações B2C (entre empresas e consumidores finais não contribuintes), aplicando percentuais fixos de retenção definidos por regulamento, com ajuste posterior. O split de contingência, previsto no §4º do Art. 32, destina-se a situações excepcionais como falhas nos sistemas de consulta, autorizando retenção integral temporária ou recolhimento direto pelo adquirente.

A implementação gradual do mecanismo está prevista na lei, com início nas operações B2C, especialmente no varejo de combustíveis, onde há maior volume de pagamentos eletrônicos (Art. 35, LC 214/2025). O Comitê Gestor do IBS e o Poder Executivo federal são responsáveis pela definição do orçamento, cronograma e infraestrutura tecnológica para a implantação.

2.2 Blockchain, Contratos Inteligentes e Gestão Pública

A tecnologia blockchain, cuja primeira prova de conceito foi apresentada por Nakamoto (2008) no paper “Bitcoin: A Peer-to-Peer Electronic Cash System”, constitui um registro distribuído onde as informações são armazenadas em blocos encadeados por criptografia hash. As propriedades fundamentais dessa tecnologia — imutabilidade, rastreabilidade e verificabilidade — decorrem de três pilares técnicos: chaves criptográficas público-privadas para autenticação, blocos com hash encadeado (tipicamente SHA-256) que criam efeito cascata em caso de alteração, e contratos inteligentes governados por protocolos de consenso que determinam as regras de validação (Freitas & Vaz, 2022).

Os contratos inteligentes, conceituados por Szabo (1997) e operacionalizados na plataforma Ethereum (Buterin, 2014), são programas autoexecutáveis armazenados na blockchain que executam automaticamente as cláusulas neles codificadas quando condições predefinidas são satisfeitas. No contexto fiscal, isso significa que

um contrato inteligente pode ser programado para, ao receber uma transação de pagamento, verificar automaticamente os dados fiscais, calcular ou validar os tributos devidos, e executar a distribuição dos valores de forma indivisível — uma operação atômica onde ou todas as transferências ocorrem simultaneamente, ou nenhuma delas ocorre.

Freitas e Vaz (2022) sistematizaram diversas iniciativas de utilização de blockchain em setores da administração pública no Brasil e no mundo, identificando experiências na saúde, registros imobiliários e prestação de contas. Dourado et al. (2023), em artigo publicado no *Journal of Technology Management & Innovation*, propuseram modelos de aplicação de blockchain fiscal especificamente para o sistema tributário brasileiro, argumentando que as características de imutabilidade e rastreabilidade da tecnologia são aderentes às necessidades de compliance fiscal. Kim (2022) ofereceu considerações normativas para formuladores de políticas públicas que deliberam sobre o uso de blockchain na administração tributária, incluindo análise de timeline, custos e riscos regulatórios. A PwC (2019) desenvolveu duas provas de conceito de blockchain para compliance tributário, demonstrando a viabilidade de pagamentos automatizados de IVA entre empresas utilizando contratos inteligentes.

2.3 A Trajetória do DREX e suas Lições para o Projeto

O DREX (Real Digital) foi um projeto do Banco Central do Brasil para a criação de uma moeda digital de banco central (CBDC). Iniciado em 2023, o projeto utilizou a plataforma Hyperledger Besu — uma implementação da Ethereum Virtual Machine (EVM) para redes permissionadas — com o módulo de privacidade Tessera para segregação de dados entre participantes. As fases piloto 1 e 2 envolveram grandes bancos (Banco do Brasil, Bradesco, Itaú, Santander, Nubank), cooperativas (Sicoob, Sicredi), e empresas de tecnologia (Microsoft, Google, AWS, Mastercard, Visa), testando tokenização de depósitos e transações com títulos públicos federais.

Em novembro de 2025, o BCB comunicou o desligamento da plataforma, considerando que a arquitetura baseada em Hyperledger Besu não atendeu aos requisitos de privacidade e segurança, além de ser financeiramente onerosa (Forbes Brasil, 2025; InfoMoney, 2025). A fase 3 do projeto, prevista para 2026, adotará uma abordagem “agnóstica quanto à tecnologia”, focando na eficiência do uso de ativos como garantia em operações de crédito, possivelmente sem blockchain (Broadcast, 2025).

Este evento é relevante para o presente trabalho por duas razões. Primeiro, ele demonstra que a escolha tecnológica deve ser consequência dos requisitos de

negócio, não o ponto de partida — lição que orienta a concepção da POC aqui apresentada como demonstração de lógica, não de plataforma. Segundo, ele evidencia que o vácuo tecnológico para infraestruturas financeiras digitais no Brasil permanece aberto, o que confere relevância a estudos que explorem alternativas arquiteturais para mecanismos como o split payment.

3. Metodologia

3.1 Abordagem Metodológica

Este trabalho adota como método a construção e validação de uma prova de conceito (PoC), abordagem consolidada na Ciência da Computação para demonstrar a viabilidade técnica de um sistema antes de sua implementação em larga escala. A PoC não pretende replicar a totalidade do sistema de split payment em ambiente de produção, mas demonstrar que a lógica de liquidação atômica com verificação criptográfica e distribuição federativa é funcional, segura e mensurável.

3.2 Arquitetura da Prova de Conceito

A arquitetura da PoC é composta por três componentes.

O primeiro componente é o Contrato Inteligente SplitPaymentBrasil, implementado em Solidity (versão 0.8.20), que modela as duas principais modalidades de split payment da LC 214/2025. Para o split padrão (Art. 32), o contrato recebe uma estrutura de dados contendo a identificação da nota fiscal, o endereço do vendedor, o valor bruto da transação, as parcelas de CBS, IBS estadual e IBS municipal, e o valor de créditos tributários a compensar. O contrato verifica a assinatura criptográfica do oráculo fiscal, checa a idempotência (se a nota fiscal já foi processada), compensa créditos tributários, recalcula a repartição proporcional entre entes federativos após a dedução de créditos, e executa quatro transferências atômicas simultâneas: vendedor (líquido), União (CBS), estado (IBS estadual) e município (IBS municipal). Para o split simplificado (Art. 33), o contrato aplica uma alíquota fixa em basis points sobre o valor bruto e direciona o total do tributo a uma conta única de conciliação para posterior repartição pelo Comitê Gestor.

O segundo componente é o Oráculo Fiscal, que simula o papel da SEFAZ e da Receita Federal. Na arquitetura proposta, o cálculo tributário é realizado off-chain pelo oráculo, que possui acesso ao motor de regras tributárias (NCM, CFOP, alíquotas por UF, regimes especiais). O oráculo assina digitalmente o pacote de dados com uma chave privada ECDSA, e o contrato inteligente verifica essa assinatura on-chain antes de executar qualquer transferência. Essa separação resolve o que denominamos “Problema do Oráculo Fiscal”: o contrato não precisa

armazenar tabelas de alíquotas (o que seria computacionalmente inviável), apenas verificar que os dados foram autorizados por uma entidade fiscal registrada.

O terceiro componente é a Suíte de Testes Unitários, implementada em JavaScript com o framework Hardhat e a biblioteca de asserções Chai. Os testes simulam uma blockchain local em memória, fazem deploy do contrato, criam contas de teste para todos os atores (comprador, vendedor, oráculo fiscal, cofres públicos) e executam cenários que verificam funcionalidade, segurança e performance.

3.3 Decisões de Design

A escolha de Solidity e do ambiente EVM para a POC não implica prescrição de plataforma. O objetivo é demonstrar a lógica de liquidação atômica em um ambiente maduro e amplamente documentado. A mesma lógica poderia ser implementada como API REST com assinatura digital e banco de dados append-only, como contrato em redes permissionadas alternativas (Corda, Fabric), ou como camada sobre a infraestrutura que o BCB definir para a fase 3 do DREX.

O uso de token ERC-20 para simular o Real Digital é uma abstração necessária para a PoC. Em ambiente de produção, o ativo tokenizado seguiria os padrões regulatórios definidos pelo BCB, com mecanismos adicionais de controle (congelamento, queima, emissão) que fogem ao escopo desta prova de conceito.

As alíquotas utilizadas nos testes (CBS: 8,65%; IBS estadual: 11,15%; IBS municipal: 4,70%; total: 24,50%) são valores ilustrativos baseados em estimativas públicas da alíquota de referência. A alíquota efetiva será definida pelo Comitê Gestor do IBS e pela Receita Federal conforme regulamentação pendente.

3.4 Cenários de Teste

Foram definidos 13 testes organizados em 8 categorias, conforme o Quadro 1.

Quadro 1 — Cenários de Teste da Prova de Conceito

| Categoria | Cenário | Artigo LC 214/2025 | O que verifica |
|------------------|----------------|---------------------------|--|
| 1. Deploy | 1.1 a 1.3 | — | Configuração correta dos cofres públicos, registro do oráculo, distribuição de saldo |
| 2. Split Padrão | 2.1 | Art. 32 | Liquidação atômica com repartição federativa (4 fluxos simultâneos) |
| 2. Split Padrão | 2.2 | Art. 32 | Emissão de evento de auditoria com dados corretos |
| 3. Créditos | 3.1 | Art. 32, §2º | Compensação de créditos tributários e retenção do tributo líquido |

| Categoria | Cenário | Artigo LC 214/2025 | O que verifica |
|------------------|----------------|---------------------------|--|
| 4. Simplificado | 4.1 | Art. 33 | Alíquota fixa B2C com envio a conta de conciliação |
| 5. Fraude | 5.1 e 5.2 | — | Rejeição de adulteração de imposto e de valor bruto |
| 6. Idempotência | 6.1 | — | Rejeição de dupla liquidação da mesma NF-e |
| 7. Autorização | 7.1 | — | Rejeição de assinatura de entidade não registrada |
| 8. Performance | 8.1 e 8.2 | — | Custo computacional (gas) do split padrão e simplificado |

Fonte: Elaboração própria (2026)

3.5 Ferramentas e Ambiente

A POC foi desenvolvida e executada com as seguintes ferramentas: Solidity 0.8.20 com compilação via IR e otimizador ativado (200 runs); OpenZeppelin Contracts v5.0 para ERC-20, AccessControl, ECDSA e MessageHashUtils; Hardhat v2.22 como framework de compilação, deploy e teste; Chai como biblioteca de asserções; Ethers.js v6 para interação com o contrato. O ambiente de execução é uma blockchain local simulada pelo Hardhat Network, sem dependência de infraestrutura externa. O código-fonte completo está disponível em repositório público <https://github.com/PSMatheus01/split-payment-poc>.

4. Resultados

4.1 Funcionalidade: Split Padrão com Repartição Federativa

O teste 2.1 demonstrou que uma transação de R\$ 1.000,00 (simulada como 1000×10^{18} wei) foi atômicamente dividida em quatro fluxos simultâneos: o vendedor recebeu R\$ 755,00 (valor líquido), a conta da União (CBS) recebeu R\$ 86,50, a conta do estado de destino (IBS estadual) recebeu R\$ 111,50, e a conta do município de destino (IBS municipal) recebeu R\$ 47,00. A soma dos quatro fluxos ($755,00 + 86,50 + 111,50 + 47,00 = 1.000,00$) foi verificada como exatamente igual ao valor bruto original, comprovando que nenhuma fração se perde na repartição.

O aspecto atômico é garantido pela natureza da transação no contrato inteligente: as quatro transferências são executadas dentro de uma única chamada de função. Se qualquer uma delas falhar (por exemplo, por saldo insuficiente), todas

são revertidas. Não existe estado intermediário onde o pagamento ao vendedor foi realizado mas o tributo não foi recolhido, eliminando estruturalmente a possibilidade de inadimplência fiscal.

4.2 Funcionalidade: Compensação de Créditos Tributários

O teste 3.1 verificou o mecanismo de compensação previsto no Art. 32, §2º da LC 214/2025. Um vendedor com R\$ 50,00 em créditos tributários acumulados teve o tributo líquido reduzido de R\$ 245,00 para R\$ 195,00. A repartição proporcional entre CBS, IBS estadual e IBS municipal foi mantida após a dedução — o contrato recalcula a fração de cada ente proporcionalmente ao tributo líquido, garantindo que a redução por compensação de créditos não altere a proporção constitucional de repartição entre entes federativos.

4.3 Funcionalidade: Split Simplificado

O teste 4.1 confirmou o funcionamento da modalidade simplificada para operações B2C. Uma venda de R\$ 200,00 com alíquota simplificada de 26,50% (2.650 basis points) resultou em retenção de R\$ 53,00, direcionados integralmente a uma conta única de conciliação, com o vendedor recebendo R\$ 147,00. Na modalidade simplificada, a repartição federativa é realizada a posteriori pelo Comitê Gestor, conforme previsto na lei.

4.4 Segurança: Rejeição de Fraude e Assinatura Não Autorizada

Os testes 5.1 e 5.2 demonstraram que a verificação criptográfica ECDSA impede qualquer adulteração nos dados fiscais após a assinatura pelo oráculo. No teste 5.1, o comprador tentou submeter a transação com o valor da CBS zerado (de R\$ 86,50 para R\$ 0,00). O contrato recalculou o hash dos dados recebidos, comparou com a assinatura, detectou a divergência e reverteu a transação com a mensagem “Assinatura fiscal inválida”. O teste 5.2 repetiu o procedimento com adulteração do valor bruto (de R\$ 1.000,00 para R\$ 500,00), obtendo o mesmo resultado.

O teste 7.1 verificou que uma assinatura produzida por uma entidade não registrada como oráculo fiscal — mesmo sendo criptograficamente válida — é rejeitada pelo contrato. O contrato recupera o endereço do signatário a partir da assinatura (via ECDSA.recover) e verifica se esse endereço possui a role FISCAL_ORACLE_ROLE. Isso demonstra que a segurança do sistema depende não apenas da criptografia, mas da governança de registro de autoridades.

4.5 Idempotência

O teste 6.1 comprovou que cada nota fiscal pode ser liquidada uma única vez. Após a primeira execução bem-sucedida, a segunda tentativa com os mesmos dados e assinatura é revertida com “NF-e já liquidada”. O mecanismo utiliza um mapeamento de hashes de notas fiscais processadas, que é atualizado atômicamente junto com as transferências.

4.6 Métricas de Performance

O Quadro 2 apresenta os custos computacionais medidos.

Quadro 2 — Custo Computacional das Modalidades de Split Payment

| Modalidade | Gas Consumido | Transferências Executadas | Verificações Realizadas |
|---|---------------|------------------------------------|--|
| Split Padrão (Art. 32) | 168.713 | 4 (vendedor + CBS + IBS-E + IBS-M) | Assinatura ECDSA + Idempotência + Créditos |
| Split Simplificado (Art. 33) | 114.268 | 2 (vendedor + conta conciliação) | Assinatura ECDSA + Idempotência |
| Transferência ERC-20 simples (referência) | ~65.000 | 1 | Nenhuma |

Fonte: Resultados da PoC (2026)

O split simplificado é 32,3% mais eficiente que o padrão, o que é explicado pela redução de duas transferências e pela ausência da lógica de compensação de créditos. Considerando que o split simplificado é direcionado a operações B2C de varejo — que representam o maior volume transacional —, a economia computacional é relevante para a escalabilidade do sistema.

O custo do split padrão (168.713 gas) equivale a aproximadamente 2,6 vezes uma transferência simples de token ERC-20, o que é razoável dado que a transação executa 4 transferências, 1 verificação ECDSA, 1 consulta de mapeamento e 1 emissão de evento com 9 parâmetros.

5. Discussão

5.1 Implicações para a Gestão Pública

Os resultados demonstram que a lógica de liquidação atômica para o split payment tributário é tecnicamente viável e apresenta propriedades que atendem diretamente às necessidades identificadas na LC 214/2025. A atomicidade garante

que o tributo seja recolhido simultaneamente ao pagamento, eliminando o gap temporal que viabiliza a inadimplência fiscal. A verificação criptográfica garante a integridade dos dados fiscais, impossibilitando a adulteração de valores entre a autorização da nota fiscal e a liquidação do pagamento. A rastreabilidade, proporcionada pelos eventos imutáveis emitidos pelo contrato, oferece uma trilha de auditoria completa e acessível em tempo real.

O modelo de Oráculo Fiscal proposto neste trabalho oferece uma separação de responsabilidades que pode ser transposta para o desenho institucional do split payment. As autoridades fazendárias (Receita Federal, SEFAZs estaduais, Comitê Gestor do IBS) mantêm a competência sobre o cálculo tributário — que envolve a complexidade de alíquotas por NCM, CFOP, regimes especiais, operações interestaduais — enquanto o sistema de liquidação apenas verifica a autorização e executa a distribuição. Isso evita a necessidade de replicar o motor de regras tributárias dentro da infraestrutura de pagamentos, reduzindo complexidade e riscos.

A compensação de créditos tributários on-chain, demonstrada no teste 3.1, é particularmente relevante para o split inteligente previsto no Art. 32. A lei determina que o sistema deve cruzar débitos e créditos do contribuinte antes de reter o tributo, retendo apenas o valor líquido. A POC demonstra que esse cruzamento pode ser realizado de forma automática e atômica, com a repartição federativa sendo recalculada proporcionalmente após a dedução de créditos.

5.2 O Abandono do Besu e a Independência de Infraestrutura

O desligamento da plataforma Hyperledger Besu pelo BCB em novembro de 2025 reforça a tese central deste trabalho: a lógica de liquidação atômica para o split payment deve ser concebida de forma independente da infraestrutura subjacente. A POC aqui apresentada utiliza Solidity e EVM como ambiente de demonstração, mas os princípios — verificação criptográfica de assinatura, liquidação atômica com múltiplos destinatários, idempotência por hash de documento fiscal, compensação de créditos — são transponíveis para qualquer plataforma que suporte assinaturas digitais e transações com múltiplas saídas.

Conforme declarou o BCB ao comunicar o encerramento da plataforma, “a escolha tecnológica deve ser consequência das necessidades do mercado, e não o ponto de partida” (Forbes Brasil, 2025). Este trabalho operacionaliza essa orientação: demonstra os requisitos funcionais e de segurança que qualquer infraestrutura para o split payment precisará atender, fornecendo uma

especificação executável que pode servir como benchmark para avaliação de plataformas candidatas.

5.3 Limitações

A POC apresenta limitações que devem ser explicitadas. Primeiro, o Oráculo Fiscal é modelado como ponto único de assinatura, quando em produção seria necessário um esquema de multi-assinatura envolvendo múltiplas autoridades fazendárias (SEFAZ de origem, SEFAZ de destino, RFB), com rotação de chaves, uso de HSM (Hardware Security Module) e certificados ICP-Brasil. Segundo, o modelo de créditos tributários é simplificado — em produção, o saldo de créditos é gerido pelo Comitê Gestor com regras complexas de apropriação, prescrição e transferência. Terceiro, a POC não modela a terceira modalidade de split payment (contingência), que envolve cenários de falha nos sistemas de consulta. Quarto, não foram realizados testes de carga em escala — o volume transacional do Brasil (da ordem de dezenas de bilhões de documentos fiscais por ano) exigiria análises de throughput que fogem ao escopo desta prova de conceito. Quinto, questões de privacidade — como o sigilo fiscal (Art. 198, CTN) e o sigilo bancário (LC 105/2001) — demandariam mecanismos de segregação de dados entre participantes que não foram implementados.

6. Considerações Finais

Este trabalho demonstrou a viabilidade técnica da utilização de contratos inteligentes para a execução do split payment tributário previsto na LC 214/2025. A prova de conceito implementou as modalidades padrão (Art. 32) e simplificado (Art. 33), demonstrando por meio de 13 testes unitários que a liquidação atômica com distribuição federativa é funcional, segura contra adulteração de dados fiscais, idempotente quanto ao processamento de notas fiscais, capaz de compensar créditos tributários, e mensurável em termos de custo computacional.

O Estado, quer do ponto de vista do estabelecimento de regulações, quer do ponto de vista da sua implementação e fiscalização, pode assumir funções importantes no desenho e na operação de sistemas como o aqui demonstrado. Conforme argumentam Freitas e Vaz (2022), a utilização de tecnologias de registro distribuído na gestão pública demanda a mobilização de capacidades tecnológicas no âmbito estatal — compreender essas tecnologias é condição para que o Estado exerça seu papel regulatório e fiscalizatório sobre a infraestrutura digital que mediará a arrecadação tributária nas próximas décadas.

A partir dos resultados do presente estudo, identificam-se caminhos para uma agenda de pesquisa. Do ponto de vista institucional, são necessários estudos sobre

os processos políticos e sociais para a definição da infraestrutura tecnológica do split payment, incluindo a governança do Comitê Gestor do IBS e as instâncias de decisão sobre padrões técnicos. Do ponto de vista tecnológico, recomenda-se a investigação de esquemas de multi-assinatura para oráculos fiscais envolvendo múltiplos entes federativos, a integração de mecanismos de privacidade (como zero-knowledge proofs ou canais privados) para atendimento ao sigilo fiscal e bancário, testes de carga em escala nacional, e estudos comparativos entre diferentes plataformas tecnológicas para a execução da liquidação atômica. A construção de um oráculo fiscal simulado como aplicação standalone e de interfaces de demonstração interativa são extensões naturais desta POC que podem ampliar sua utilidade como instrumento de diálogo entre academia, governo e setor financeiro.

7. Referências

AGÊNCIA BRASIL. Brasil perde R\$ 417 bi por ano com sonegação de impostos, diz estudo.

Agência Brasil, Brasília, 12 dez. 2020. Disponível em:

<https://agenciabrasil.ebc.com.br/geral/noticia/2020-12/brasil-perde-r-417-bi-por-ano-com-sonegacao-de-impostos-diz-estudo>. Acesso em: 10 fev. 2026.

AINSWORTH, R. T.; SHACT, A. Blockchain (Distributed Ledger Technology) Solves VAT Fraud. **Boston University School of Law, Law and Economics Research Paper**, n. 16-41, 2016.

AINSWORTH, R. T.; MUSAAD, A. Real Time VAT Collection Using Blockchain Technology. **Boston University School of Law**, 2017.

BRASIL. Emenda Constitucional nº 132, de 20 de dezembro de 2023. Altera o Sistema Tributário Nacional. **Diário Oficial da União**, Brasília, 2023.

BRASIL. Lei Complementar nº 214, de 16 de janeiro de 2025. Institui o Imposto sobre Bens e Serviços (IBS), a Contribuição Social sobre Bens e Serviços (CBS) e o Imposto Seletivo (IS). **Diário Oficial da União**, Brasília, 2025. Disponível em:

https://www.planalto.gov.br/ccivil_03/leis/lcp/lcp214.htm. Acesso em: 10 fev. 2026.

BRASIL. Ministério da Fazenda. Split Payment e Reforma Tributária: um salto para a modernidade fiscal. **Portal Gov.br**, 30 mai. 2025. Disponível em:

<https://www.gov.br/fazenda/pt-br/assuntos/noticias/2025/Maio/split-payment-e-reforma-tributaria-um-salto-para-a-modernidade-fiscal>. Acesso em: 10 fev. 2026.

BUTERIN, V. A Next-Generation Smart Contract and Decentralized Application Platform. **Ethereum White Paper**, 2014.

COMISSÃO EUROPEIA. Analysis of the Impact of the Split Payment Mechanism as an Alternative VAT Collection Method. **Final Report**, Directorate-General for Taxation and Customs Union, dez. 2017. Disponível em:

https://taxation-customs.ec.europa.eu/system/files/2018-01/split_payment_report_execsummary_2017_en.pdf. Acesso em: 10 fev. 2026.

DOURADO, L. V. N. et al. Application Models for a Fiscal Blockchain: The Brazilian Tax System. **Journal of Technology Management & Innovation**, v. 18, n. 3, p. 19-30, 2023. Disponível em: <https://www.scielo.cl/scielo.php?pid=S0718-27242023000300019>. Acesso em: 10 fev. 2026.

FORBES BRASIL. Banco Central abandona o blockchain do Drex, o projeto do “Real Digital”. **Forbes Brasil**, 4 nov. 2025. Disponível em: <https://forbes.com.br/escolhas-do-editor/2025/11/banco-central-abandona-o-blockchain-do-drex-o-projeto-do-real-digital/>. Acesso em: 10 fev. 2026.

FREITAS, A. R.; VAZ, J. C. Potenciais aplicações e benefícios na utilização de sistemas blockchain para a gestão pública. **Boletim de Políticas Públicas/OIPP**, n. 20, mar. 2022. Disponível em: <https://sites.usp.br/boletimoipp/marco-de-2022/>. Acesso em: 10 fev. 2026.

INFOMONEY. BC desliga plataforma do DREX usada até agora por problemas de segurança. **InfoMoney**, 4 nov. 2025. Disponível em: <https://www.infomoney.com.br/minhas-financas/bc-suspendera-plataforma-drex-permanentemente-por-falta-de-seguranca-dizem-fontes/>. Acesso em: 10 fev. 2026.

KIM, Y. Blockchain Initiatives for Tax Administration. **UCLA Law Review**, v. 69, n. 1, 2022. Disponível em: <https://www.uclalawreview.org/wp-content/uploads/securepdfs/2022/07/Kim-69-1.pdf>. Acesso em: 10 fev. 2026.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 10 fev. 2026.

PWC. Two Practical Cases of Blockchain for Tax Compliance. **PwC Netherlands**, 2019. Disponível em: <https://www.pwc.nl/nl/tax/assets/documents/pwc-two-practical-cases-of-blockchain-for-tax-compliance.pdf>. Acesso em: 10 fev. 2026.

RECEITA FEDERAL DO BRASIL. Gap Tributário do IRPJ/CSLL: Relatório 2015-2019. **Portal Gov.br**, 2023. Disponível em: <https://www.gov.br/receitafederal/pt-br/centrais-de-conteudo/publicacoes/estudos/tax-gap/>. Acesso em: 10 fev. 2026.

SZABO, N. Formalizing and Securing Relationships on Public Networks. **First Monday**, v. 2, n. 9, 1997.

VALOR ECONÔMICO. BC decide desligar plataforma do Drex e abre caminho para mudança tecnológica. **Valor Econômico**, 4 nov. 2025. Disponível em: <https://valor.globo.com/financas/criptomoedas/noticia/2025/11/04/banco-central-decide-desligar-plataforma-do-drex.ghtml>. Acesso em: 10 fev. 2026.

VERTEX INC. VAT Compliance Update, Part 2: Split Payment. **Vertex Inc.**, 18 out. 2019. Disponível em: <https://www.vertexinc.com/resources/resource-library/vat-compliance-update-part-2-split-payment>. Acesso em: 10 fev. 2026.