PILOTO DREX

RELATÓRIO

fase 1

BANCO CENTRAL DO BRASIL

PILOTO DREX

RELATÓRIO

fase 1

BANCO CENTRAL DO BRASIL

Sumário

Introdução

A tokenização de ativos e moedas tem despertado grande interesse entre os bancos centrais ao redor do mundo. Muitos deles, representando quase a totalidade do Produto Interno Bruto (PIB) global, estão investigando, explorando ou testando projetos, aspectos operacionais e tecnológicos de sistemas de tokenização.

Nesse ponto, é importante definir o termo "tokenização" conforme será utilizado neste relatório. Esse conceito ainda está sendo desenvolvido pelos definidores internacionais de princípios para o setor financeiro. As minutas mais recentes do Banco de Compensações Internacionais (Bank for International Settlements – BIS) tendem a convergir para a seguinte definição:

- **tokenização** – refere-se ao processo de criar e registrar uma representação digital de ativos tradicionais em uma plataforma programável. Esse conceito envolve dois componentes principais, *tokens* digitais e plataformas programáveis. *Tokens* digitais são entradas em um banco de dados que podem conter informações e funcionalidades, representando ativos. As plataformas programáveis permitem que participantes elegíveis desenvolvam e executem aplicações que atualizam um livro-razão comum, como a Tecnologia de Registro Distribuído (DLT). A interrelação entre *tokens* digitais e plataformas programáveis forma arranjos de *tokens*, que possibilitam a execução de funções de mercado financeiro, como emissão, negociação e liquidação de transações.

Nossa visão para a evolução dos *tokens* dentro da Plataforma Drex pode ser dividida em três estágios:

- ***Token* Estágio 1 – Representação do Valor** – neste estágio, os *tokens* representam o valor dos ativos de forma digital;
- ***Token* Estágio 2 – Incorporação da Inteligência de Negócio** – aqui, os *tokens* começam a incorporar funcionalidades de negócios, permitindo operações mais complexas;
- ***Token* Estágio 3 – Incorporação da Componibilidade** – neste estágio, os *tokens* são altamente componíveis, permitindo a criação de novos produtos e serviços financeiros de forma modular.

As Moedas Digitais de Banco Central (*Central Bank Digital Currency* – CBDCs), tokenizadas, ancoram financeiramente o sistema a um passivo do banco central, permitindo a utilização plena e democrática da tecnologia. Nesse sentido, a tokenização pode melhorar a eficiência dos serviços financeiros e de pagamentos de varejo, além de promover a competição e a inclusão financeira para a população com pouco ou nenhum acesso a serviços bancários.

Outra definição importante a ser feita é para o termo "Drex", que pode ter diferentes significados dependendo do contexto:

- **Projeto Drex** – refere-se ao projeto corporativo do Banco Central do Brasil (BC) que trata das fases de implantação da Plataforma Drex;
- **Plataforma Drex** – conjunto de regras, procedimentos e estrutura operacional para o processamento e liquidação de transações financeiras em conjunto com o ecossistema financeiro que o cerca. Engloba, mas não se limita ao conceito de Sistema do Mercado Financeiro (SMF);
- **Piloto Drex** – fase do Projeto Drex com características de laboratório em que a plataforma é testada em ambiente de desenvolvimento com participantes selecionados, sem a participação de cidadãos ou empresas externas ao piloto;
- **Drex de Atacado** – CBDC cuja titularidade é controlada pela Plataforma Drex. O Drex de Atacado é emitido pelo BC a favor das instituições com acesso direto a contas e passivo digital da autarquia. Equivale a versões tokenizadas das disponibilidades em Reservas Bancárias (RB), Contas de Liquidação (CL) e Conta Única do Tesouro Nacional;
- **Drex de Varejo** – moeda digital emitida pelas instituições financeiras (IFs) ou pelas Instituições de Pagamento (IPs) cuja titularidade é controlada pela

Plataforma Drex. Para atingir os principais objetivos da implantação do Real Digital, é importante manter a intermediação financeira e a capacidade de alavancagem e de geração de crédito do sistema bancário. Assim, mantém-se o foco de uso para as transações de varejo, especificando que o acesso a clientes finais, pessoas naturais e pessoas jurídicas não financeiras deve se dar por meio de moedas digitais emitidas por agentes autorizados pelo BC, ou seja, versões tokenizadas de depósitos à vista em IFs e de moedas eletrônicas em IPs.

Diretrizes da Plataforma Drex

As diretrizes da Plataforma Drex foram estabelecidas por meio do Voto 31/2023-BCB, de 14 de fevereiro de 2023, e visam orientar o desenvolvimento e a operação da Plataforma Drex. As principais diretrizes são:

- **Inovação Tecnológica** – desenvolvimento de modelos inovadores incorporando tecnologias como contratos inteligentes (*smart contracts*) e dinheiro programável, compatíveis com a liquidação de operações por meio da Internet das Coisas (IoT);
- **Aplicações *On-line* e *Off-line*** – foco no desenvolvimento de aplicações *on-line*, mantendo a possibilidade de pagamentos *off-line*;
- **Emissão do Drex de Atacado** – o BC emite o Drex de Atacado como meio de pagamento, permitindo a oferta de serviços financeiros de varejo liquidados pelo Drex de Varejo emitido por participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB);
- **Normas e Regras** – aplicação das normas e regras atuais para operações realizadas na Plataforma Drex, evitando assimetrias regulatórias;
- **Segurança Jurídica** – garantia da segurança jurídica nas operações realizadas na Plataforma Drex;
- **Privacidade e Segurança** – garantia dos princípios e regras de privacidade e segurança previstos na legislação brasileira, especialmente na Lei do Sigilo Bancário (Lei Complementar 105, de 10 de janeiro de 2001) e na Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei 13.709, de 14 de agosto de 2018);
- **Prevenção a Ilícitos** – desenho tecnológico que atenda integralmente às recomendações internacionais e normas legais sobre prevenção à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa, incluindo o cumprimento de ordens judiciais para rastreamento de operações ilícitas;

- **Tecnologia DLT** – adoção de solução tecnológica baseada em DLT que permita:
  - » registro de ativos de diferentes naturezas;
  - » descentralização no provimento de produtos e serviços;
  - » interoperabilidade com sistemas domésticos legados e outros sistemas de registro e transferência de informação e negociação de ativos digitais regulados; e
  - » integração com sistemas de outras jurisdições para a realização de pagamentos transfronteiriços.
- **Resiliência e Segurança Cibernética** – adoção de padrões de resiliência e segurança cibernética equivalentes aos aplicáveis a infraestruturas críticas do mercado financeiro.

1 A Fase I do Piloto Drex

1.1. Privacidade, programabilidade e descentralização: trilema

Dentre as diretrizes estabelecidas para a Plataforma Drex, está a adoção de uma plataforma DLT com capacidade de registrar ativos de diferentes naturezas e que possibilite o provimento descentralizado de novos produtos e serviços através da criação e composição de contratos inteligentes, observando as regras de privacidade estabelecidas pelo arcabouço regulatório brasileiro.

Com esses requisitos, surge o desafio de criar produtos e serviços em uma rede descentralizada com sistemas de privacidade avançados.

Sistemas centralizados, como o Sistema de Transferência de Reservas (STR) e o Sistema de Pagamentos Instantâneos (SPI), dependem de uma instituição central para armazenar dados e processar operações. O controlador do sistema mantém as informações em um ambiente restrito e aplica regras rigorosas de acesso, permitindo que apenas os proprietários dos ativos consultem suas posições e realizem operações.

Em 2009, a DLT eliminou a necessidade de um controlador central único. A proposta é que uma rede colaborativa processe transações e guarde a posição de cada participante. O banco de dados é descentralizado e replicado, com cada participante possuindo uma cópia completa e tendo acesso direto a todas as informações. Todas as operações são validadas por um conjunto de participantes, não por um controlador central.

No cenário de redes DLTs, a privacidade é diferente. A nova tecnologia expõe participantes, transações e saldos a qualquer membro da rede. A identificação é feita por pseudoanonimato, utilizando um par de chaves criptográficas para dissociar contas das identidades reais dos usuários. A chave pública identifica a conta, enquanto a chave privada movimenta os ativos nela depositados.

Com o pseudoanonimato, a privacidade depende da dificuldade de vincular números de contas às identidades reais. Embora isso nem sempre seja simples e direto, é possível, especialmente com o uso de ferramentas analíticas sobre os dados compartilhados.

Observa-se que as soluções atuais de privacidade para DLT utilizam técnicas que geralmente tratam apenas da propriedade e movimentação de ativos de forma sigilosa, validando a autenticação das partes e protegendo contra a criação de ativos sem permissão ou o envio de ativos sem lastro. Essas técnicas permitem uma simples transferência de propriedade de um ativo de forma sigilosa.

Entretanto, a criação de regras mais complexas, como as codificadas em contratos inteligentes, torna-se inviável quando as informações necessárias para sua execução estão ocultas. Em uma rede Ethereum, para que uma transação seja considerada válida pela rede, os contratos são executados pelos validadores que verificam se as regras escritas no código são respeitadas. Adicionalmente, os validadores garantem a autenticação das partes e a existência de saldo para honrar as transações. Assim, se as informações estão ocultas por técnicas de criptografia, como as regras e informações podem ser verificadas pelos validadores?

Com base nesse problema, estabeleceu-se como principal objetivo do Piloto Drex testar soluções tecnológicas de privacidade, avaliando seu grau de maturidade, aderência ao arcabouço regulatório e capacidade de viabilizar a criação e composição de serviços por meio de contratos inteligentes.

1.2. Escopo do Piloto Drex

O Piloto Drex é a fase de testes para operações com a moeda digital brasileira. Nessa etapa, o Banco Central avalia os benefícios da programabilidade suportada pela Plataforma Drex, um ecossistema multiativos onde serão simuladas operações com ativos digitais (“tokenizados”). É importante destacar que nenhum teste do Piloto Drex envolve clientes ou ativos reais; todos os clientes e ativos utilizados são fictícios.

O principal desafio nesta fase inicial do piloto é equilibrar a privacidade das transações financeiras, conforme preconizado Lei do Sigilo Bancário,, com a programabilidade e a descentralização.

Ressalta-se que, para o piloto, não foi realizada a integração com nenhum sistema externo ao Drex. Não obstante, convém mencionar que tal integração será indispensável para a futura disponibilização dos serviços em produção para efeitos de controle, segurança e contabilização, tanto pelo BC como pelo sistema externo. A estratégia foi focar e priorizar os recursos no que traria maior valor de aprendizado da tecnologia DLT, bem como viabilizar o cronograma de execução pretendido.

Possíveis participantes do Piloto Drex

- **Instituições autorizadas** com acesso direto a contas e passivo digital do BC.
- **Usuários finais simulados**, que realizarão transações de varejo por meio do Drex, na sua forma digital ("tokenizada") de saldos em reais mantidos em instituições financeiras (depósitos à vista) ou de pagamento (moeda eletrônica).
- **Secretaria do Tesouro Nacional (STN)** com a emissão de Títulos Públicos Federais (TPF) e a liquidação de transações envolvendo esses títulos com Entrega contra Pagamento (*Delivery versus Payment* – DvP) no nível do cliente final.

1.3. Requisitos Básicos para os Testes do Piloto Drex

- ***Ledger* Unificado (*Unified Ledger*)**: uso de plataforma baseada em DLT para controle da titularidade de ativos de diferentes naturezas (multiativo) e contraprestações a eles atreladas.
- ***Tokens***: representação de depósitos das contas RB, de Contas de Liquidação e da Conta Única do Tesouro Nacional; de depósitos bancários à vista; de contas de pagamento de instituições de pagamento; e de TPF. Serão mantidos os critérios de acesso às contas RB ou de Liquidação, conforme a disciplina legal e regulatória vigente.
- **Chaves**: as chaves dos usuários foram custodiadas por um participante designado, responsável por garantir sua segurança. Essa abordagem foi escolhida para assegurar a integridade e a proteção dos ativos dos usuários finais (empresas e cidadãos), proporcionando uma camada adicional de confiança.
- **Transações**: emissão, resgate, transferência de ativos e fluxos financeiros decorrentes de eventos de negociação. As transações contemplarão a liquidação condicionada entre os *tokens* para garantir o DvP ou o Pagamento contra Pagamento (PvP) em toda a cadeia da componibilidade (liquidação

atômica). O controle da titularidade dos ativos e o histórico das transações deverão possibilitar fragmentação, respeitando o sistema de apreçamento centesimal, para ampliar um dos benefícios potenciais da tecnologia DLT.

- **Funcionalidades essenciais**: camadas de controle de titularidade de ativos, de liquidação em tempo real de suas transações e de contratos inteligentes necessários para a execução das funcionalidades propostas no Piloto Drex. Não será permitido saldo a descoberto em nenhuma transação.

1.4. Participantes Selecionados para o Piloto Drex

O BC recebeu 36 propostas de interesse na participação no Piloto Drex, anteriormente conhecido como o Projeto-Piloto da Plataforma do Real Digital (Piloto RD). Essas propostas vieram de mais de cem instituições de diversos segmentos financeiros, incluindo candidaturas individuais e consórcios de entidades.

O Comitê Executivo Gestor (CEG) do Piloto Drex, com base nos critérios estabelecidos no Regulamento do Piloto Drex, selecionou dezesseis propostas, listadas a seguir por ordem de inscrição:

- **Bradesco, Nuclea e Setl;**
- **Nubank;**
- **Banco Inter, Microsoft e 7Comm;**
- **Santander, Santander Asset Management, F1RST e Toro CTVM;**
- **Itaú Unibanco;**
- **Basa, TecBan, Pinbank, Dinamo, Cresol, Banco Arbi, Ntokens, Clear Sale, Foxbit, CPqD, AWS e Parfin;**
- **Caixa, Elo e Microsoft;**
- **SFCoop: Ailos, Cresol, Sicoob, Sicredi e Unicred;**
- **XP, Visa;**
- **Banco BV;**
- **Banco BTG;**
- **Banco ABC, Hamsa, LoopiPay e Microsoft;**
- **Banco B3, B3 e B3 Digitas;**
- **Consórcio ABBC: Banco Brasileiro de Crédito, Banco Ribeirão Preto, Banco Original, Banco ABC Brasil, Banco BS2 e Banco Seguro, ABBC, BBChain, Microsoft e BIP;**
- **MBPay, Cerc, Sinqia, Mastercard e Banco Genial;**
- **Banco do Brasil.**

Essa seleção inclui representantes de instituições financeiras dos Segmentos Prudenciais S1 a S4 , instituições de pagamento, cooperativas, bancos públicos, desenvolvedores de serviços de criptoativos, operadores de infraestruturas de mercado financeiro e instituidores de arranjos de pagamento.

O BC iniciou a incorporação dos participantes à plataforma do Piloto Drex em julho de 2023 e finalizou essa primeira fase em outubro de 2024.

1.5. Casos de uso

Os testes realizados introduzem inovações em relação aos casos de negócio atualmente vigentes no SFN e no SPB, principalmente em dois aspectos.

Primeiro, a Plataforma Drex, de forma distribuída e padronizada, integra os saldos detidos por clientes nas instituições autorizadas a funcionar pelo BC e seus saldos em TPF. Atualmente, esses registros são mantidos nos sistemas internos das próprias instituições ou no Sistema Especial de Liquidação e de Custódia (Selic). Com o controle desses saldos pela Plataforma Drex, os clientes finais podem usufruir dos ganhos de eficiência e do desenvolvimento de novos negócios realizados nesse sistema.

Segundo, a Plataforma Drex permite a liquidação final e irrevogável de transferências e compras de TPF entre clientes que não são participantes diretos dos SMF aplicáveis. Atualmente, essa liquidação é realizada no nível das instituições participantes diretas dos SMF, enquanto a liquidação das posições dos clientes é feita nos livros desses participantes diretos.

Essas inovações têm o potencial de aumentar a eficiência e a segurança das transações dos clientes.

Neste capítulo, analisaremos casos de uso de três tipos de *tokens*: Drex de Atacado, Drex de Varejo e Título Público Federal Tokenizado (TPFt). No escopo do piloto, esses *tokens* foram selecionados, cada um com seus casos de uso específicos, para abordar o trilema entre descentralização, programabilidade e privacidade.

Inicialmente, os casos de uso foram implementados considerando apenas as dimensões de descentralização e programabilidade, sem incluir a dimensão de privacidade. Em uma segunda etapa de testes, a dimensão de privacidade foi incorporada, abrangendo todos os casos de uso e *tokens*.

A seguir, detalharemos cada tipo de *token* e seus casos de uso.

1.5.1. Drex de Atacado

Nesta seção, apresentamos o desenvolvimento dos processos de negócio relacionados aos *tokens* de RB e de CL, denominados Drex de Atacado.

Foi estabelecido que cada R$ 1 nas contas RB ou CL corresponderia a uma unidade de Drex de Atacado, garantindo uma conversão direta e simples entre o dinheiro tradicional e a versão tokenizada.

Assim, o Drex de Atacado foi estruturado em três processos essenciais:

- emissão de *Tokens* de Drex de Atacado;
- transferência de *Tokens* de Drex de Atacado;
- conversão de *Tokens* de Drex de Atacado de volta para RB/CL.

a. Emissão de *tokens* de Drex de Atacado

Dado o escopo do piloto não incluir integrações com sistemas externos, o Drex de Atacado foi emitido na Plataforma Drex sem considerarmos a necessidade de lançar a contraparte nas contas da instituição no STR ou no SPI.

Nesse sentido, o BC forneceu os meios para simular a conversão de saldos das contas RB ou CL em *tokens* de Drex de Atacado a fim de se fazer o devido aporte diretante na carteira do solicitante.

Observa-se, portanto, que não existe a possibilidade de débito na conta RB ou CL de uma instituição para emissão de Drex de Atacado para uma terceira instituição.

Ademais, o BC (por meio de interface *web*) criou meios para acompanhar o trabalho das instituições, assim como para emitir os seus próprios *tokens*, utilizando para isso "instituições virtuais de teste do BC", para fins de testes internos.

Ressalta-se, por fim, que o processo de emissão de Drex de Atacado é mutuamente condicionado à sensibilização das contas RB ou CL. Assim, apenas ocorre a emissão do Drex de Atacado para a instituição solicitante se ocorrer o débito simulado do respectivo valor em conta RB ou CL.

b. Transferência de *tokens* de Drex de Atacado

Esse processo consiste na transferência de Drex de Atacado entre duas instituições participantes da rede Drex.

Vale destacar que essa transferência ocorre sem afetar, em sistemas externos, as contas RB/CL das instituições envolvidas, mas variações nas posições em Drex de Atacado deveriam, em ambiente produtivo, ser refletidas nos sistemas contábeis de cada instituição no BC.

A operação de transferência deve ser comandada pela instituição que está transferindo o Drex de Atacado, isso é, a instituição titular que está cedendo os *tokens*.

Esse processo é considerado atômico, o que significa que ele deve ser concluído de forma integral, sem falhas. Em outras palavras, o crédito de Drex de Atacado na instituição de destino só ocorre se o débito correspondente for realizado na instituição de origem, garantindo a integridade da transação.

c. Queima ou conversão de *tokens* de Drex de Atacado de volta em RB/CL

Este processo é a operação inversa à descrita no item "a". Nele, o Drex de Atacado existente na carteira da instituição é debitado (ou queimado), resultando em um crédito correspondente, simulado, na conta RB ou CL dessa instituição.

De forma análoga ao item "a", não é possível queimar Drex de Atacado de uma instituição para creditar diretamente a conta de uma terceira instituição.

Assim como os processos anteriores, esta operação também possui as características de um processo mutuamente condicionado.

d. Resultado e avaliação de negócio

Os testes realizados com os dezesseis consórcios participantes, além da STN, validaram com sucesso os processos de emissão, transferência e queima de Drex de Atacado.

Todos os consórcios executaram com sucesso os fluxos, sem exceção, resultando no levantamento realizado ao final da primeira iteração da primeira fase do piloto, antes do início dos testes das soluções com privacidade, em um total de mais de 420 operações distintas de emissão de Drex de Atacado, 450 transferências e 130 queimas de Drex de Atacado.

Nota-se que a liquidação das transações ocorreu de forma bruta em tempo real (LBTR), com *finality* e garantia de PvP , sem permitir saldo a descoberto e respeitando o princípio da atomicidade das operações.

1.5.2. Drex de Varejo

Nesta seção, apresentamos o desenvolvimento dos processos de negócio relacionados aos *tokens* de Depósitos à Vista (DVt) e de Moedas Eletrônicas (MEt) mantidos em contas (ou "carteiras") das instituições participantes do Drex.

Foi definido que cada R$ 1 em depósito à vista ou moeda eletrônica seria convertido em uma unidade de Drex de Varejo, garantindo uma correspondência direta e uma transição simples e transparente e entre o dinheiro tradicional e sua versão digital.

Desde o início do piloto, foram acordados alguns pontos do Drex de Varejo que ficariam fora do escopo da primeira fase:

- bloqueios administrativos e contratuais sobre os DVt e MEt;
- estornos de lançamentos incorretos em DVt e MEt;
- cobrança de tarifas dos clientes pela emissão, transferência e resgate de DVt e MEt;
- aspectos da relação contratual entre o depositante e a instituição financeira ou de pagamento sobre a prestação de serviços de manutenção da carteira digital, emissão e transferência de DVt e MEt;
- débitos automáticos, DDA sobre valores em DVt e MEt;
- cobranças de valores pela IF depositária em relação a débitos em atraso, com uso do saldo de DVt e de MEt do cliente depositante;
- questões relativas ao compulsório sobre o saldo em DVt e dos depósitos em TPF para MEt; e
- aspectos relativos ao curso legal (art. 1º, da Lei 9.069, de 29 de junho de 1995) do DVt/MEt, obrigando que um cliente receba valores em DVt ou MEt.

Além disso, alguns processos essenciais foram identificados, mas optou-se por deixá-los fora do escopo da primeira fase devido às limitações de tempo e à complexidade. Entre esses processos, destacam-se:

- o bloqueio judicial pelo Sisbajud poderá alcançar o DVt/MEt do cliente;
- a produção de informações de contas e carteiras individualizadas, para atender à legislação e solicitações do Poder Judiciário;

- as operações em DVt/MEt devem gerar relatórios e documentos hábeis para manter os registros gerenciais, contábeis e de acompanhamentos atualmente vigentes para as contas de depósito à vista e contas de pagamento pré-pagas; e
- o cadastro do cliente (depositante) deverá seguir os dispositivos vigentes para abertura, manutenção e encerramento de conta e será realizado pela instituição financeira ou instituição de pagamento.

Na primeira fase do piloto Drex, a tokenização dos depósitos à vista e das moedas eletrônicas foi estruturada em quatro processos essenciais:

- emissão de Drex de Varejo, de forma descentralizada pelas instituições;
- transferência em Drex de Varejo, entre clientes da mesma instituição;
- transferência em Drex de Varejo, para cliente de outra instituição;
- conversão de Drex de Varejo, de volta para depósito à vista ou moeda eletrônica na instituição.

a. Emissão de Drex de Varejo de Forma Descentralizada pelas Instituições

Esse processo consiste na emissão de *tokens* DVt pelas instituições participantes do Piloto Drex a partir de depósitos à vista mantidos em contas transacionais por seus clientes finais. As instituições também emitem *tokens* MEt, da mesma forma, com base nos saldos de moedas eletrônicas de seus clientes finais mantidos em seus registros.

Ressalta-se a natureza descentralizada das emissões, em que cada instituição participante emite seus próprios *tokens* de Drex de Varejo para seus clientes finais, que são os titulares dos ativos.

Apesar dessa descentralização, o BC se capacitou para monitorar os processos relacionados ao Drex de Varejo (por meio de interfaces *web*), permitindo o acompanhamento dos testes realizados no piloto.

Além disso, assim como na emissão do Drex de Atacado, a emissão de *tokens* DVt e MEt é um processo mutuamente condicionado. A instituição emissora deve garantir a equivalência entre as emissões de DVt e MEt e os correspondentes débitos nos saldos de depósitos à vista e de moedas eletrônicas dos seus clientes finais nos sistemas externos. Nesse caso, à sua escolha, ou a instituição realiza os débitos em ambiente de testes, usando contas e clientes finais virtuais, ou utiliza artifícios de simulação como aqueles empregados no caso do Drex de Atacado, apenas simulando o registro dos débitos em contas, sem fazê-los de fato.

b. Transferência em Drex de Varejo entre clientes da mesma instituição

A transferência entre clientes da mesma instituição é uma operação conhecida como transferência intrabancária. Nela, o montante de Drex de Varejo emitido por uma instituição transita entre clientes finais da própria instituição, conforme as regras e as características definidas no Drex.

Nesse contexto, é possível que ambas as pontas de uma operação específica utilizem DVt ou MEt, ou que uma ponta utilize DVt e a outra MEt.

Por se tratar de um processo atômico, a instituição responsável pela transferência do Drex de Varejo deve assegurar que o crédito ao cliente destinatário somente será efetivado se o débito ao cliente remetente também ocorrer, e vice-versa.

c. Transferência em Drex de Varejo para cliente de outra instituição

Esta operação é conhecida como transferência interbancária, pois envolve duas instituições: uma de origem, com o cliente pagador, e outra de destino, com o cliente recebedor. Entre elas, há um sistema de troca de reservas, que, no caso em questão, é a liquidação da posição de Drex de Atacado realizada por meio do Drex para compensar o Drex de Varejo transferido entre as instituições envolvidas. A Figura 1 abaixo ilustra o caso.

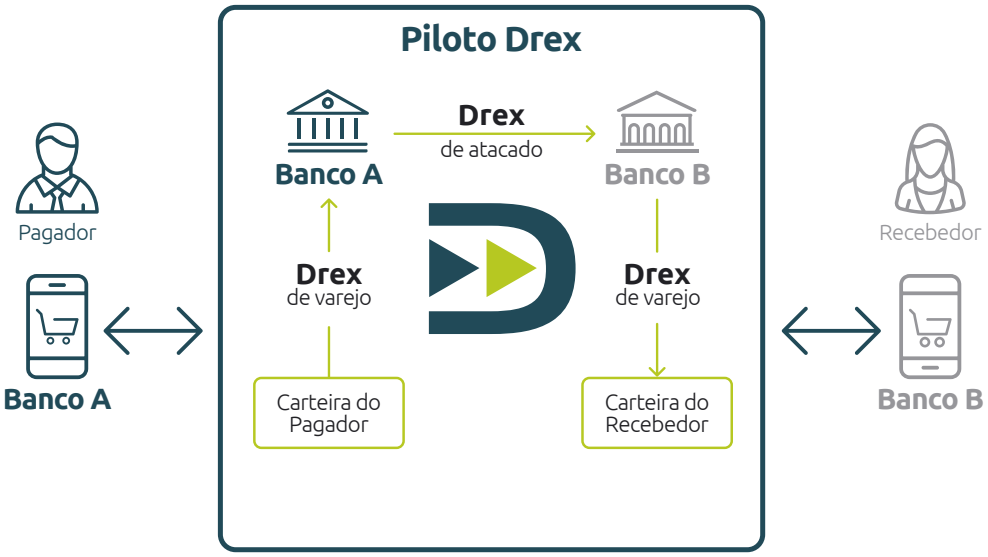

Figura 1

O cliente recebedor deve receber o Drex de Varejo da sua instituição, pois pode não ter relacionamento com a instituição de origem ou, por qualquer motivo,

não ter interesse em receber recursos atrelados à última. Para que a operação seja concretizada, a instituição de origem deve queimar os *tokens* na quantidade a ser transferida, enquanto a instituição de destino deve emitir novos *tokens*, de valor equivalente, para o cliente recebedor.

Adicionalmente, para que a operação seja concluída, a instituição do cliente pagador deve possuir o valor equivalente em Drex de Atacado, uma vez que esse montante será transferido para a instituição do cliente recebedor para compensar a operação entre as instituições envolvidas.

Assim, em resumo, o processo envolve: queima do Drex de Varejo na instituição pagadora, transferência de Drex de Atacado da instituição pagadora para a instituição recebedora, e emissão de Drex de Varejo na instituição recebedora.

Destaca-se que o fluxo descrito no parágrafo anterior constitui, como um todo, um processo atômico, que deve ser concluído de maneira integral e sem falhas. O Drex deve garantir que, uma vez concluída qualquer etapa do processo, todas as demais também sejam finalizadas. Se ocorrer falha irreparável em algum ponto, deve-se garantir que nenhuma outra etapa seja concluída.

Nos termos do parágrafo anterior, tem-se uma operação envolvendo três diferentes ativos (o Drex de Atacado e dois diferentes Drex de Varejo), em que há garantia, ponta a ponta, até os clientes finais, de PvP.

d. Conversão de Drex de Varejo para depósito à vista ou moeda eletrônica na instituição

Esse processo é a operação inversa à descrita no item "a". Nele, o Drex de Varejo depositado na instituição é debitado (ou queimado), resultando em um crédito correspondente, real ou simulado, na conta de depósito à vista ou em moeda eletrônica na instituição participante em um sistema externo, conforme o caso.

Essa operação é mutuamente condicionada, ou seja, a conversão só é considerada concluída quando a queima do DVt e o crédito do depósito à vista, ou a queima do MEt e o crédito na conta de moeda eletrônica, ocorrem ambos de forma garantida. A instituição que emitiu os *tokens* é a responsável por dar essa garantia.

e. Resultado e avaliação de negócio

Os testes realizados com os dezesseis consórcios participantes validaram com êxito os processos de emissão, transferência intrabancária e interbancária, além da queima de Drex de Varejo.

Todos os consórcios executaram com sucesso os fluxos definidos, sem exceções. Na avaliação feita ao final da primeira iteração da primeira fase do Piloto, antes do início dos testes das soluções de privacidade, foram contabilizadas mais de 1.900 operações distintas de emissão de Drex de Varejo, trezentas transferências intra-bancárias, 1.600 transferências interbancárias e 1.700 queimas de Drex de Varejo.

Vale destacar que, conforme monitorado durante os testes, as instituições participantes atenderam, dentro das possibilidades desta primeira iteração, aos requisitos estabelecidos para a emissão e a gestão de seus *tokens*. Em especial, as transferências interbancárias atômicas cumpriram os requisitos de LBTR, *finality* e PvP, com o Drex de Atacado atuando como intermediário nas trocas dos Drex de Varejo das instituições.

1.5.3. Título Público Federal Tokenizado

Nesta seção, descrevemos o desenvolvimento dos processos de negócio relacionados ao TPFt, que foi escolhido para exercitar nesta fase do piloto as transações financeiras com contraprestação e, com isso, possibilitar a avaliação mais abrangente da tecnologia e dos pilares de programabilidade, descentralização e privacidade.

De acordo com a diretriz do piloto, que, na definição dos requisitos do TPFt, estabelece que a tecnologia não altera a estrutura jurídica do ativo implementado, o BC e o STN buscaram preservar os requisitos essenciais do negócio relacionado aos títulos, permitindo ajustes operacionais para aproveitar ao máximo a tecnologia. Além disso, procurou-se desconsiderar premissas e limitações que fossem exclusivas de títulos federais, como o impedimento de operações de TPFt entre clientes.

No Selic, o BC é responsável pelos processos de emissão, liquidação de leilões, colocações diretas e resgates dos títulos nele custodiados, conforme delegação da STN. Durante o exercício do piloto, essa delegação de atribuições foi reproduzida.

Na primeira fase do piloto Drex, a tokenização dos TPF foi estruturada em seis processos essenciais:

- emissão de *tokens* de TPFt;
- operação de colocação direta;
- operação de liquidação de oferta pública;
- operação de compra e venda;
- transferência sem financeiro; e
- operação de resgate.

Nesse sentido, o BC simulou os processos de emissão, colocação direta e de leilão de oferta pública para fornecer títulos tokenizados aos participantes do piloto. Foi criada uma interface *web* (*overledger*) para realizar esses comandos, executando o contrato da operação na rede e passando os parâmetros de cada operação comandada pelo BC.

a. Emissão de *tokens* de TPFt

Dentro da estratégia de priorização e foco na tecnologia DLT foi decidido que, para fins do piloto, não haveria conversão de TPF em TPFt. Com isso, foi realizado um processo de emissão de *tokens* de novos títulos diretamente na rede DLT.

A operação de emissão foi desenvolvida como um comando único pelo BC representando a STN. Os *tokens* de TPFt são emitidos exclusivamente na carteira da STN e transferidos para as carteiras dos participantes por meio de colocação direta ou liquidação de oferta pública.

A emissão é um processo atômico, que deve acontecer por completo, do início ao fim.

b. Operação de colocação direta

Operação pela qual a STN ordena a colocação de títulos diretamente na carteira de um beneficiário específico, sem contrapartida financeira no Selic e sem realização de oferta pública.

No âmbito do piloto, esse processo foi estabelecido como a transferência de uma quantidade inteira de TPFt da carteira da STN para a carteira de uma instituição participante da rede Drex, sem contrapartida financeira.

A operação deve ser comandada pelo BC, em comando único, representando a STN.

A colocação direta é um processo atômico, que deve acontecer por completo, do início ao fim.

c. Operação de liquidação de oferta pública

A negociação por oferta pública corresponde ao mercado primário de títulos. Consiste em um leilão em que a STN emite uma portaria ofertando determinada quantidade de títulos ao mercado financeiro, em condições específicas, a ocorrer em determinada data e horário, por meio do sistema Oferta Pública Formal Eletrônica (Ofpub), um dos módulos complementares do Selic. Nesse sistema, as instituições financeiras apresentam propostas em resposta à oferta da STN.

Encerrada a fase de propostas, ocorre a seleção, a divulgação dos resultados e, por fim, a liquidação das propostas vencedoras.

Para fins do piloto, foi estabelecido que apenas a etapa de liquidação seria exercitada, partindo de um resultado fictício pré-estabelecido em que cada um dos consórcios participantes teria propostas vencedoras.

A operação de liquidação de oferta consiste na transferência de quantidades inteiras de TPFt da carteira da STN para a carteira do participante, conjugada com a transferência de financeiro do participante para a carteira da STN.

Nota-se que a liquidação da operação é realizada com o DvP, utilizando o fluxo de transferência do Drex de Atacado, transferindo uma quantidade de Drex de Atacado da carteira do participante para a carteira da STN. As carteiras devem possuir saldo no momento da transação.

A operação é de duplo comando e deve ser realizada pelo BC, representando a STN, que vai entregar os TPFt, e pelo participante responsável pela proposta vencedora, que entregará o valor financeiro em Drex de Atacado.

A operação de liquidação de oferta pública é considerada atômica, o que significa que ela deve ser concluída de forma integral, sem falhas, garantindo a integridade da transação. Em outras palavras, o DvP implica que o crédito de TPFt na carteira do comprador só ocorre se o crédito de Drex de Atacado correspondente for realizado na carteira do vendedor.

d. Operação de compra e venda

Operação de compra e venda de TPFt corresponde ao mercado secundário de títulos. Essas operações são realizadas com quantidades inteiras ou fracionárias, em que ocorre a transferência tanto de TPFt como de financeiro (Drex de Atacado e/ou Drex de Varejo).

A operação é de duplo comando e deve ser realizada pelos participantes envolvidos. O participante transmite o comando para suas carteiras e para as carteiras de seus clientes. Vale destacar que o cliente não interage diretamente com a rede DLT, sendo representado pelo participante que lhe presta o serviço de custódia.

A liquidação da operação ocorre com DvP, envolvendo entrega de TPFt e entrega de financeiro nas carteiras envolvidas. Quando envolve participantes distintos,

há liquidação em Drex de Atacado e, quando envolve cliente, há liquidação em Drex de Varejo. Em qualquer caso, o DvP implica que todas as transferências envolvidas são realizadas ou nenhuma é feita.

Os seguintes cenários são possíveis:

i. **compra e venda entre dois participantes** – o DvP consiste em um processo atômico composto pela transferência dos TPFt da carteira do participante vendedor para a carteira do participante comprador e na transferência de Drex de Atacado no sentido oposto;
ii. **compra e venda entre dois clientes do mesmo participante** – o DvP consiste em um processo atômico composto pela transferência dos TPFt da carteira do cliente vendedor para a carteira do cliente comprador e na queima de Drex de Varejo na carteira do comprador com a correspondente emissão de Drex de Varejo na carteira do vendedor;
iii. **compra e venda entre um participante e um cliente seu** – o DvP consiste em um processo atômico composto pela transferência de TPFt entre a carteira do participante e a carteira do seu cliente, e na queima/emissão de Drex de Varejo na carteira do cliente;
iv. **compra e venda entre um participante e um cliente de participante distinto** – o DvP consiste em um processo atômico composto por três passos, sendo (1) a transferência de TPFt entre a carteira do participante e a carteira do cliente do participante distinto; (2) a queima/emissão de Drex de Varejo na carteira do cliente; e (3) a transferência de Drex de Atacado entre os participantes;
v. **compra e venda entre clientes de participantes distintos** – o DvP consiste em um processo atômico composto por quatro passos, ilustrados pela Figura 2, sendo (1) a transferência de TPFt da carteira do cliente vendedor para a carteira do cliente comprador; (2) a queima de Drex de Varejo na carteira do cliente comprador; (3) a transferência de Drex de Atacado do participante do cliente comprador para a carteira do participante do cliente vendedor; e (4) a emissão de Drex de Varejo na carteira do cliente vendedor.

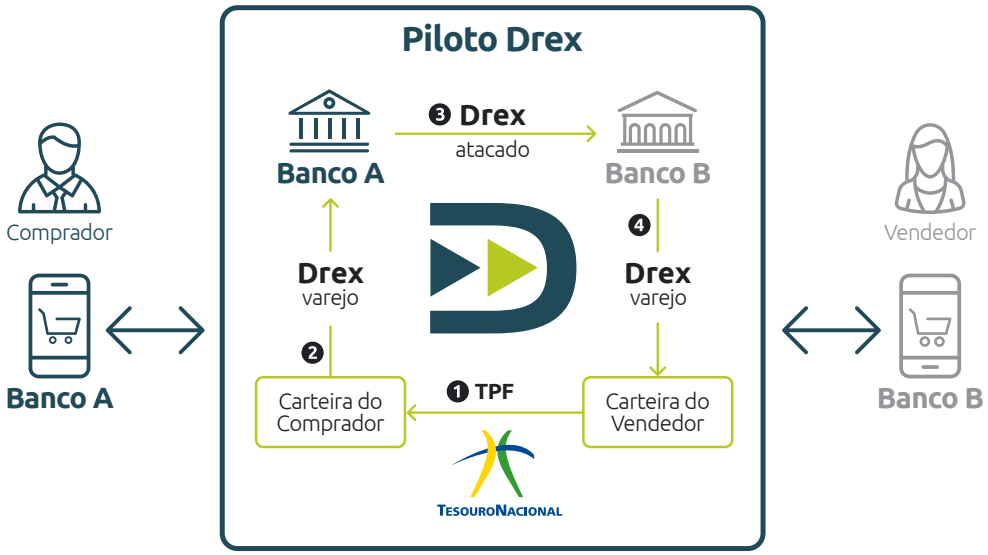

Figura 2

Destaca-se que o contrato inteligente referente à compra e venda de TPFt faz uso dos contratos inteligentes de Drex de Atacado e Drex de Varejo, exercitando a componibilidade.

e. Transferência sem financeiro

Essa funcionalidade permite que o TPFt seja transferido sem que haja troca financeira, ou seja, uma quantidade de TPFt sai da carteira de origem e é transferido para a carteira de destino. Neste caso, o comando é único e é enviado somente pela carteira de origem.

f. Operação de resgate

O processo de resgate, que é relativamente simples em sistemas centralizados, apresentou complexidade maior que o esperado com a tecnologia DLT, revelando-se como uma excelente oportunidade de aprendizado, como será descrito a seguir.

O resgate consiste no pagamento final do título pela STN, que ocorre em sua data de vencimento e encerra-se com a baixa do título. No Selic, durante o processamento *off-line*, é gerada automaticamente uma operação de resgate para cada conta em que houver títulos em custódia cuja data de vencimento coincida ou que seja anterior ao dia útil seguinte. Um dos requisitos considerado essencial para o resgate é que este ocorra, independentemente de qualquer ação por parte do detentor do título. Há raros casos de exceção em que a conta de custódia de títulos não possui um participante correspondente para quem possa ser realizado

o pagamento automaticamente – nesses casos, o resgate é efetuado, mas o pagamento é realizado para uma conta financeira do BC que, satisfeitas determinadas condições pelo interessado, realiza o pagamento de forma não automatizada.

Inicialmente, os primeiros testes do resgate foram realizados com a tentativa de efetuar o pagamento para cada carteira com custódia do TPFt com vencimento no dia útil seguinte, inclusive carteiras de cliente, em transação atômica, ou seja, ou todos os passos seriam feitos ou nenhum deles seria realizado. Não obstante, essa prática não se mostrou a mais adequada no piloto, especialmente pelo caso de carteiras de cliente às quais o BC não dispunha de acesso para fazer pagamentos, situação que se mostrou mais frequente do que se imaginava no decorrer dos testes. Neste ponto, vale recordar que utilizar as prerrogativas de BC para forçar o pagamento independentemente de autorização iria inviabilizar conclusões aplicáveis a *tokens* cuja autoridade não fosse o BC. Sendo assim, a fragilidade do procedimento revelou-se na necessidade de os participantes concederem autorização para todas as carteiras com saldo de TPFt, inclusive as carteiras de clientes. Considerou-se que seria provável tais falhas ocorrerem em situações reais.

Diante disso, foi projetado outro modelo de resgate para o exercício no piloto:

- **carteira de participante** – paga-se em Drex de Atacado na carteira do participante e, em caso de falha, paga-se na carteira padrão do participante;
- **carteira de cliente** – paga-se em Drex de Atacado na carteira padrão do participante e em Drex de Varejo na carteira do cliente. Em caso de falha no pagamento da carteira do cliente, caberá ao próprio participante fazer o pagamento em Drex de Varejo, reiterando-se que o participante já terá recebido o pagamento equivalente em Drex de Atacado.

Nos casos em que não for possível o pagamento para a carteira padrão do participante, que se estima como muito raro, o pagamento em Drex de Atacado será feito para um contrato, que ficará responsável pelos resgates remanescentes.

Com o pagamento realizado, seja para o participante/cliente ou para contrato, o TPFt é queimado/baixado, constituindo o resgate numa transação atômica, ou seja, todos os passos são feitos ou nada é feito.

Ocorrendo pagamentos para o contrato, caberá ao interessado solicitar o pagamento devido, informando a carteira onde estavam custodiados os TPFt. Daí, automaticamente, o contrato fará o pagamento para a carteira solicitada, sendo esta transação atômica.

Nesse modelo, também exercitado nos testes, preserva-se o requisito essencial de que o resgate ocorra independentemente de ação dos participantes e, nos avaliados como raros casos de impossibilidade de pagamento, ainda se obtém a vantagem da automatização do procedimento de pagamentos remanescentes. Destaca-se que, no estudo dos ajustes normativos necessários ao Drex, esse modelo de funcionamento do resgate é um assunto a ser avaliado.

g. Testes realizados

Os testes realizados com os dezesseis consórcios participantes validaram com sucesso os processos de emissão, colocação direta, liquidação de oferta pública, compra e venda, transferência e resgate de TPFt.

A liquidação das transações ocorreu em tempo real, de forma final e irrevogável, com garantia de DvP, sem permitir saldo a descoberto e respeitando o princípio da atomicidade das operações.

Foram realizadas, nesta primeira fase, 1.263 operações liquidadas com sucesso, sendo:

- 9 operações de emissão de TPFt;
- 131 operações de colocação direta;
- 33 liquidações de oferta pública;
- 184 operações de compra e venda entre os participantes;
- 862 operações de compra e venda com clientes; e
- 44 resgates.

Foram emitidas 25 milhões de Letras do Tesouro Nacional (LTN) e seis milhões de Letras Financeiras do Tesouro (LFT) para que as operações pudessem ser testadas.

2 Arquitetura

2.1. Critérios de seleção da plataforma

Considerando a visão de longo prazo da Plataforma Drex e as diretrizes para desenvolvimento do piloto, optou-se por validar o uso de uma plataforma Ethereum Virtual Machine (EVM) em uma rede permissionada que possibilitasse a incorporação de protocolos já implementados no ambiente público Ethereum, buscando maximizar os ganhos de programabilidade e avaliar a viabilidade de aderência ao regramento vigente, especialmente no que diz respeito ao sigilo bancário e à Lei Geral de Proteção de Dados Pessoais.

A plataforma selecionada para o Piloto Drex foi a Ethereum Hyperledger Besu, com base nos seguintes critérios:

- plataforma EVM para rede permissionada;
- suporte a certo grau de privacidade para avaliação inicial da aderência a requisitos regulatórios;
- projeto suportado pela comunidade Hyperledger, *open source* e com desenvolvimento ativo, possibilitando evolução e inovação contínua;
- existência de fornecedores de tecnologia da informação (TI) certificados que asseguram suporte técnico diversificado;
- plataforma já utilizada em projetos em produção no mundo.

2.2. Infraestrutura

2.2.1. Rede Drex

A rede DLT privada do Piloto Drex é composta por 26 nós Hyperledger Besu, na versão 24.1.1, sendo dez no BC e dezesseis nos participantes. Dentre os dez nós administrados pelo BC, seis desses nós validam transações e blocos, enquanto os outros quatro respondem a chamadas JavaScript Object Notation-Remote Procedure Call (JSON-RPC) de aplicações internas, sem participar do consenso para novos blocos.

Os dezesseis nós restantes, que não são validadores, são administrados pelos participantes do piloto. Todos os 26 nós da rede Drex estão interligados por meio da Rede do Sistema Financeiro Nacional (RSFN)[1].

Como requisito para conexão à rede do Piloto Drex, exigiu-se que cada instituição financeira ou consórcio tivesse uma largura de banda mínima disponível de 6 Mbps, de forma redundante, em seus *links Multiprotocol Label Switching* (MPLS) da RSFN, de forma garantir a acomodação de tráfego advindo da sincronização dos blocos quando do ingresso na rede e dos testes de carga de cem transações por segundo (TPS) promovidos ao longo do piloto sem impacto para os demais serviços prestados à sociedade.

A Figura 3 abaixo resume como estão distribuídos os nós da rede Drex, em que as dezesseis instituições participantes estão representadas de maneira exemplificativa, nas figuras dos participantes A, B, C e D.

1 A RSFN é a estrutura de comunicação de dados que tem por finalidade amparar o tráfego de informações no âmbito do SFN para serviços autorizados, conforme Circular 3.970, de 28 de novembro de 2019.

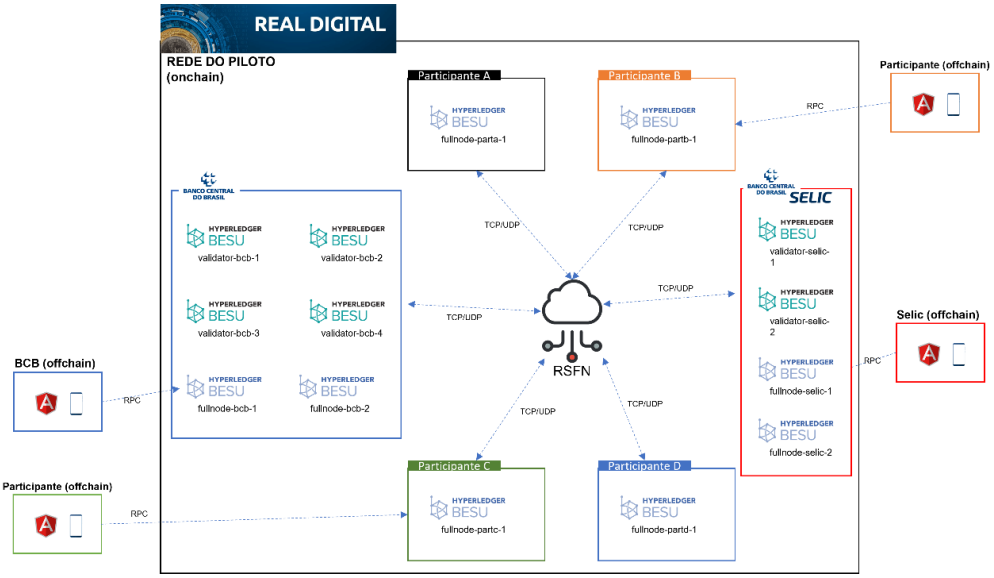

Figura 3

Nota-se que a comunicação entre os nós ocorre na camada de transporte da RSFN (Protocolo de Datagrama de Usuário – UDP/Protocolo de Controle de Transmissão – TCP). Já os serviços *off-chain* de cada membro, para leitura e envio de transações, fazem acesso ao nó local via JSON-RPC. Assim, no âmbito do piloto, não há intercâmbio de informações entre participantes fora da camada 1 do *blockchain*.

2.2.2. Topologias adotadas

Na arquitetura inicial da rede DLT do Piloto Drex, todos os nós estavam configurados para realizar a descoberta automática (*discovery*) dos demais membros da rede, sem restrições na quantidade de conexões iniciadas ou recebidas por cada nó.

Essa configuração se traduz em conexão total entre os membros, o que promove uma arquitetura robusta e tolerante a falhas por habilitar o intercâmbio direto de dados e transações entre quaisquer pares de nós. No entanto, embora esse arranjo seja bastante resiliente, resulta em elevado consumo de banda de rede, proporcional à quantidade de participantes interconectados.

Como alternativa, o BC optou por alterar a topologia da rede DLT do piloto para uma composição tipo estrela, em que os membros não validadores da rede (*fullnodes*), administrados pelo BC e pelos participantes, deixam de conectar-se entre si e comunicam-se apenas com os nós validadores. Estes, por sua vez, interconectam-se por meio de uma rede *full mesh*.

A estrutura em estrela é viabilizada definindo-se configuração estática de quais nós os *fullnodes* devem se conectar, isto é, uma lista exaustiva com os endereços dos validadores é utilizada como referência para conexão, ao passo que os nós de validação executam em modo *discovery* habilitado e, portanto, conectam-se a todos os nós da rede.

Após a alteração da topologia, o consumo de banda nos nós não validadores deixou de ser proporcional ao número de participantes. Isso permite a inclusão de novos membros sem a necessidade de ampliar a largura de banda mínima disponível para conexão à rede do piloto. Na seção dos testes de desempenho, pode-se perceber a redução no consumo de banda de rede por parte dos participantes após a adoção da topologia em estrela.

2.2.3. Motivação para uso da RSFN

Devido ao risco tecnológico e de segurança inerentes aos testes do Piloto Drex, o BC decidiu que o acesso à plataforma seria exclusivamente pela RSFN, sem acesso pela internet.

O uso da RSFN reduz significativamente a possibilidade de acessos não autorizados, pois um agente malicioso precisaria primeiro comprometer uma instituição conectada à essa rede e, mesmo dentro dessa instituição, acessar ativos relacionados aos serviços dela.

Por outro lado, o dimensionamento adequado dos *links* de acesso e a exigência de uma banda mínima para a participação no piloto visam proteger os serviços atualmente disponíveis à sociedade que utilizam a RSFN.

2.2.4. Infraestrutura no BC

No BC, a infraestrutura do Piloto Drex está implantada em tecnologia de nuvem privada distribuída em quatro *datacenters*: dois localizados na cidade de Brasília/DF e outros dois situados no Rio de Janeiro/RJ. Os *datacenters* na mesma cidade comunicam-se entre si por *links* dedicados. Já os *datacenters* nas diferentes cidades utilizam a RSFN para a comunicação. A Figura 4 a seguir detalha a implantação da plataforma sob administração do BC.

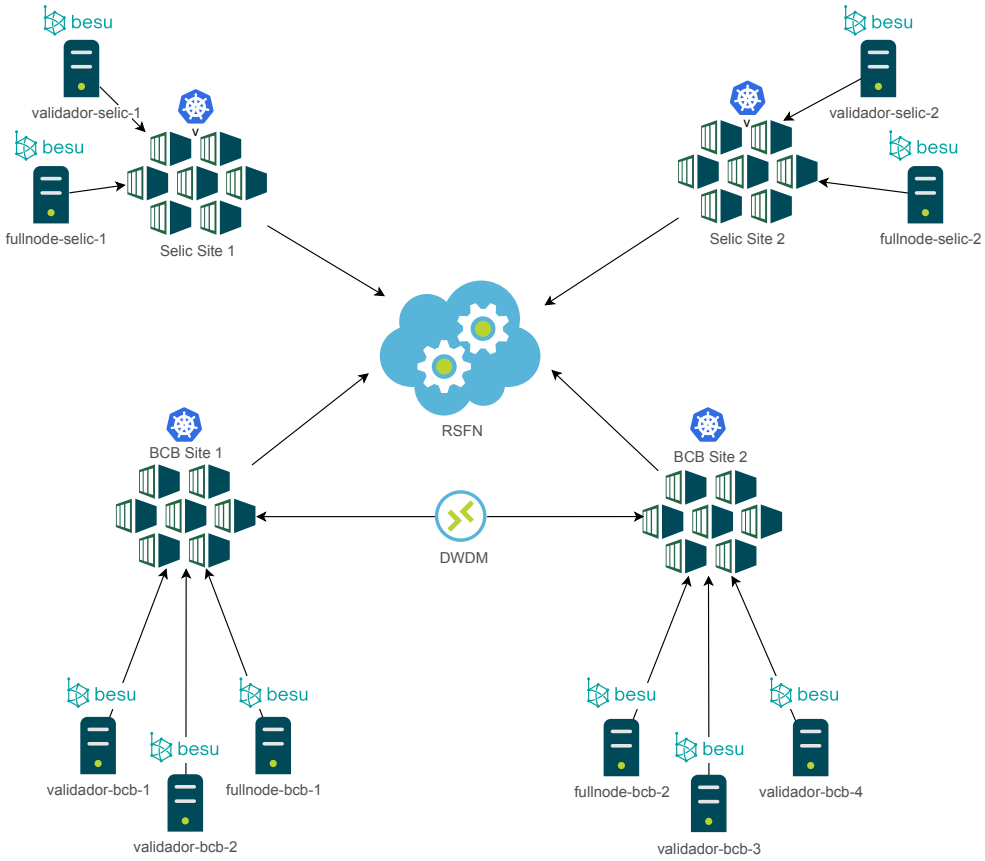

Figura 4

2.2.5. Protocolo de consenso

Utiliza-se como protocolo de consenso o *Quorum Byzantine Fault Tolerant* (QBFT), em que seis nós atuam como validadores e, portanto, revezam entre si na proposição do próximo bloco da rede, configurada para geração de cinco em cinco segundos. O QBFT é o protocolo recomendado para uso corporativo em redes privadas e está permanentemente sob avaliação e melhoria por parte dos grupos colaboradores e mantenedores da comunidade Hyperledger Besu.

Como redes QBFT exigem que os blocos sejam assinados pela supermaioria (2/3) dos validadores antes de serem inseridos na rede, estes seis nós estão distribuídos fisicamente de modo a oferecer resiliência para a falha de um dos *datacenters*, isto é, a indisponibilidade de qualquer uma das quatro localidades de processamento não provoca interrupção na geração de blocos pela rede. Por outro lado, a rede oferece capacidade para tolerar mau funcionamento ou comportamento malicioso de um dos nós validadores ((n-1) /3), sendo "n" o número de validadores da rede.

À medida que a rede Drex evolua ou ganhe criticidade, pretende-se estender o papel de validador para outros participantes, a fim de promover maior descentralização e robustez ao serviço tanto do ponto de vista de tolerância à falha operacional (*crash fault tolerance*) quanto à falha bizantina[2] (*byzantine fault tolerance*) dos membros.

O número de validadores, no entanto, não deve exceder dezesseis para evitar um tempo muito prolongado de consenso. Estudos difundidos na comunidade especializada mostram que, acima desse número de membros votantes, a quantidade de mensagens de validação torna-se grande o suficiente para reduzir sensivelmente a capacidade da plataforma, além do aumento da latência das transações.

2.2.6. Permissionamento de nós e contratos

O Hyperledger Besu oferece suporte a configurações de quais nós podem se conectar à rede (node permissioning) e de quais contas Ethereum podem enviar transações para os nós membros (account permissioning).

Na rede Drex, as duas opções de permissionamento são adotadas utilizando-se contrato inteligente para o registro de nós e contas autorizadas. Assim, a administração do acesso está centralizada, sob o controle do BC.

Vale ressaltar que parte das configurações de permissionamento são realizadas localmente em cada nó e, portanto, não é possível garantir a configuração correta. Assim, existe a possibilidade de um nó, uma vez autorizado *on-chain*, desabilitar a configuração local e permitir que outros nós não permissionados se conectem à rede utilizando-se deste nó ou que realizem transações, o que pode levar a conexões não autorizadas ou vazamento de informações.

Também é possível configurar contas Ethereum autorizadas a enviar transações. Embora essa configuração também possa ser desabilitada localmente pelo membro participante, o impacto para a segurança da rede é menor, uma vez que transações de contas não autorizadas seriam propagadas pelo nó discordante, mas seriam rejeitadas por todos os outros nós da rede por inconformidade de permissionamento.

Como medida adicional de segurança, adaptou-se o contrato inteligente que promove o cadastramento de contas autorizadas na rede a fim de se restringir o escopo

2 A Tolerância a falhas bizantinas se refere ao “Problema dos Generais Bizantinos”, que descreve a dificuldade que grupos descentralizados têm em chegar a um consenso sem depender de uma parte central confiável. Sistemas com tolerância a falhas bizantinas respondem à questão de como seus membros conseguem concordar coletivamente sobre uma ocorrência em uma rede onde nenhum membro consegue verificar a identidade dos outros.

de contratos elegíveis para execução de transações. Assim, somente contratos inteligentes previamente registrados numa lista criada e mantida pelo operador da plataforma é que podem ser invocados.

2.2.7. Testes de desempenho

No intuito de avaliar possíveis alterações de desempenho ao longo da construção e evolução do piloto, a equipe técnica exercitou cenários de testes submetendo os nós membros a processamento de cargas da ordem de 100 TPS.

Os testes aconteceram, sobretudo, antes e depois de alguma modificação relevante no ambiente de modo a avaliar os impactos da alteração e, portanto, não se propunham a exaurir a capacidade máxima da rede.

Utilizou-se como ferramentas o Ethereum Benchmark e o Hyperledger Caliper para geração de carga de transações. Os parâmetros de desempenho de interesse investigados foram o consumo de banda dos links RSFN de nós participantes, indicadores de latência e de taxa de transferência da rede, além do consumo de recursos computacionais dos nós (Unidade Central de Processamento – CPU, memória, *input/output* – I/O).

Alterações de configuração no âmbito da plataforma, como evolução de versão do Hyperledger Besu e do protocolo de rede, não trouxeram variações de desempenho relevantes. Por outro lado, os testes realizados para avaliar a modificação na topologia da rede, de full mesh para arranjo tipo estrela, revelam resultados de melhoria nos indicadores de desempenho das transações e de redução no tráfego de rede.

Os resultados de latência, em regra, baixaram após a alteração de topologia, ao passo que o taxa de transferência apresentou melhora quase nula. Do ponto de vista do consumo de banda rede, a mudança para a topologia em estrela reduziu sensivelmente a troca de mensagens entre os nós, o que se refletiu na ocupação de banda dos *links* de rede de dados. Os *links* do BC experimentaram redução de, pelo menos, 22%, enquanto houve participante que divulgou diminuição de, no mínimo, 35% no tráfego de dados.

Por fim, ainda que não fosse a proposta principal do estudo de desempenho realizado, a equipe técnica conduziu testes exploratórios para avaliar a capacidade atual da rede Drex. Os achados dos testes revelam que, nas configurações e topologia ora apresentadas, a rede manifesta condições de absorver cargas de 125 TPS sem que haja comprometimento dos demais serviços disponíveis na RSFN.

Adicionalmente, registra-se que a exploração acima não visou identificar possíveis gargalos e solucioná-los para aumento de capacidade, uma vez que a Plataforma Drex está em construção e depende dos testes com soluções de privacidade, que possuem suas particularidades e possíveis restrições adicionais.

3 Privacidade

3.1. Detalhamento dos requisitos de privacidade pretendidos

a. A autoridade sobre o *token* deve possuir acesso à consulta de todas as operações realizadas com o *token* e os saldos de *token* de todas as carteiras, respeitando as normas de privacidade e segurança estabelecidas.
b. A autoridade sobre o *token* deve ser capaz de transferir total ou parcialmente o saldo de *token* de qualquer carteira, exclusivamente em casos excepcionais previstos em lei, regulamentação ou contrato, e mediante registro detalhado da operação.
c. A autoridade sobre o *token* deve ser capaz de implementar o resgate independentemente de qualquer ação do detentor do *token*, em casos previstos, mediante registro detalhado da operação.
d. Os participantes que não estão envolvidos na transferência de um *token* não devem ter acesso a essa informação, garantindo a confidencialidade e a integridade dos dados transacionados.

3.2. Arquiteturas de privacidade

3.2.1. Prova de conhecimento zero

A Prova de Conhecimento Zero (ZKP) baseia-se em um conjunto de protocolos criptográficos que permitem a uma parte (o "provador") provar à outra parte (o "verificador") que uma determinada afirmação é verdadeira sem revelar qualquer

informação adicional além da veracidade da própria afirmação. Essa tecnologia tem aplicações importantes na computação remota confiável, especialmente no contexto do Piloto Drex e suas necessidades de privacidade em uma rede descentralizada.

No Piloto Drex, a ZKP pode permitir que os participantes da rede comprovem que possuem atributos específicos para realizar operações, sem precisar revelar informações sensíveis sobre si mesmos ou os dados envolvidos na operação. Por exemplo, um participante pode provar que possui uma determinada quantidade de ativos digitais sem revelar quais ativos possui ou seu histórico de transações.

Embora a ZKP seja um conceito relativamente antigo na criptografia, recentemente houve um crescimento de investimentos e desenvolvimento no campo da ZKP. Impulsionada por avanços em pesquisa e desenvolvimento, bem como pela crescente demanda por privacidade e segurança em diversos setores, a ZKP está se tornando uma tecnologia cada vez mais viável e acessível. No entanto, apesar desse cenário de rápida expansão, é possível observar que nem todas as soluções em desenvolvimento possuem a maturidade e a qualidade necessárias para serem aplicadas em sistemas críticos como o Drex. A adoção prematura de tecnologias ZKP pode expor o sistema a riscos e vulnerabilidades imprevistas, comprometendo a segurança e a confiança na rede. É fundamental, portanto, que o Drex adote uma abordagem criteriosa na seleção e na implementação de soluções ZKP, priorizando tecnologias maduras, testadas e com histórico comprovado de segurança, apesar dos significativos benefícios potenciais em termos de privacidade, segurança e confiança na rede que justificam a investigação e o desenvolvimento de soluções baseadas em ZKP.

3.2.2. Segregação de redes

Arquiteturas de segregação de redes baseiam-se na criação de múltiplas redes interconectadas, cada uma com suas características e suas especializações. Esse modelo permite que diferentes tipos de transações e dados sejam processados em segmentos separados simultaneamente e segundo suas regras de privacidade.

A segregação de redes em camadas é amplamente utilizada em sistemas DLT. Em geral, a camada 1 é uma *blockchain* pública ou compartilhada por um consórcio que serve como garantia de imutabilidade das transações nas camadas superiores. Em seguida, várias redes de camada 2 podem ser construídas utilizando a camada 1 para ancoragem de confiança[3], depósito de provas ou canal de comunicação. Essas redes podem ser projetadas para lidar com transações ou conjuntos de dados

3 Ancoragem de confiança: técnica utilizada na web3, em que uma rede deposita periodicamente uma prova criptográfica sucinta do seu estado global em outra rede, teoricamente mais confiável.

específicos, oferecendo maior privacidade e escalabilidade. As redes de camada 3, se presentes, podem fornecer funcionalidades adicionais ou personalizações para casos de uso específicos, ancorando sua confiança em uma rede de camada 2, e assim por diante.

A segregação em redes oferece diversas vantagens, como a capacidade de implementar mecanismos de privacidade distintos por rede. Além disso, a escalabilidade pode ser aprimorada, pois as camadas 2 e 3, se possuírem acesso direto a todos os ativos transacionados, podem processar um grande volume de transações em paralelo, sem a necessidade de envolver imediatamente a camada 1. A modularidade da arquitetura permite a inovação e a experimentação com novas tecnologias sem comprometer a segurança da rede principal.

No entanto, essa abordagem também apresenta desafios, como a complexidade de gerenciar e integrar múltiplas redes, além da necessidade de garantir a interoperabilidade e a comunicação segura entre elas. A governança do sistema se torna mais complexa, exigindo a coordenação entre os diferentes participantes e a definição de regras claras para a interação entre sistemas e redes. A programabilidade com ativos em redes diferentes depende das mesmas estratégias de coordenação e comunicação utilizadas em sistemas centralizados. Além disso, a programabilidade é prejudicada pela segregação, pois um contrato não consegue acessar ativos em redes distintas para compor um sistema coeso. À medida que o número de camadas aumenta ou quando há um alto grau de dependência entre elas, a comunicação torna-se mais complexa e lenta, impactando negativamente os possíveis ganhos de escalabilidade.

3.2.3. Computação confidencial

A computação confidencial busca garantir a execução segura de programas em computadores remotos, sejam eles confiáveis ou não, assegurando a integridade e a confidencialidade dos dados processados. Essa área de pesquisa está alinhada aos desafios do Piloto Drex para cumprir os requisitos legais de privacidade em uma rede descentralizada, pois permite o isolamento de dados sensíveis em ambientes de execução protegidos (Trusted Execution Environment – TEE).

Durante o Piloto Drex, a equipe analisou soluções de ambientes de execução protegidos com suporte a processadores Intel e AMD.

As soluções de computação confidencial avaliadas baseiam-se em uma raiz de confiança definida em seu processo de manufatura que utiliza, para cada processador, uma chave segura exclusiva. O processador cria um ambiente seguro, geralmente

composto por uma área de memória e processamento protegida do restante da CPU, impedindo que agentes não autorizados acessem as informações de execução do programa ou os dados processados, garantindo, assim, a integridade da execução e a privacidade das informações.

Optou-se por não adotar a arquitetura nos testes do piloto, especialmente devido à:

- **interoperabilidade** – soluções de segurança em *hardware* dependem de funções de baixo nível que não seguem uma padronização, resultando em incompatibilidade entre fabricantes, dependência de um único fornecedor e impossibilidade de migração;
- **segurança –** há risco de o processador não executar as instruções conforme as especificações, permitindo a existência de *backdoors*. A auditoria é dificultada pela criptografia, cuja chave é acessível apenas ao processador, dificultando a detecção de comportamentos anômalos. As implementações de computação confidencial avaliadas exigem que os fabricantes insiram chaves criptográficas nos processadores durante a fabricação para criptografar os dados e realizar o atesto remoto[4]. O vazamento dessas chaves permitiria que um agente malicioso se apresentasse como um sistema confiável no atesto, comprometendo sua integridade, ou possibilitaria que um atacante decifrasse os dados estacionários ou em trânsito sem o conhecimento do proprietário. O ponto mais crítico é a dificuldade de detecção do vazamento, pois não há evidências de falhas na execução do trabalho computacional;
- **descentralização –** o piloto Drex pressupõe um ambiente descentralizado para a provisão e execução serviços, onde os nós da rede têm visibilidade e participação nos processos, garantindo conjuntamente a correta execução dos serviços. Entretanto, com computação confidencial, o ambiente se torna mais centralizado. O BC passaria a ser o proprietário do código e dos dados, enquanto os participantes, responsáveis pela execução remota, forneceriam apenas capacidade de processamento e energia elétrica, sem participação ou visibilidade sobre o processo de computação.

3.2.4. Privacidade por controle de acesso

Neste cenário, a rede *blockchain* é restrita às autoridades, como o BC. Os participantes do sistema financeiro, como bancos e outras instituições, interagem com a rede por meio de Interfaces de Programação de Aplicativos (APIs) fornecidas por

4 O atesto remoto é um processo na computação confidencial que fornece evidências da confiabilidade do sistema ao proprietário do trabalho computacional antes que dados confidenciais sejam enviados para processamento no ambiente seguro, garantindo que ninguém possa alterar os dados ou o *software* nesse ambiente.

essas autoridades. Embora essa abordagem seja mais centralizada, ela oferece vantagens, como maior controle para as autoridades, facilitando a implementação de políticas e a garantia da conformidade. Além disso, a segurança é aprimorada ao reduzir a superfície de ataque e minimizar riscos. A privacidade é incorporada desde o início, com APIs projetadas para fornecer acesso apenas aos dados estritamente necessários, e a flexibilidade das APIs permite sua adaptação às necessidades específicas sem a necessidade de modificar a rede *blockchain* subjacente e vice-versa.

No entanto, a maior centralização também apresenta desafios, como preocupações sobre a autonomia dos participantes e uma menor tolerância a falhas da rede como um todo. A dependência das APIs fornecidas pelas autoridades pode limitar a inovação e a programabilidade. A implementação e o gerenciamento de APIs seguras, robustas e auditáveis são essenciais para garantir a segurança e a privacidade dos dados, bem como a flexibilidade e a adaptabilidade do sistema às necessidades em constante evolução do sistema financeiro.

A fim de preservar o requisito de um ambiente descentralizado, a arquitetura não foi adotada nos testes do Piloto Drex.

3.3. Soluções de privacidade testadas

Durante o processo de seleção das soluções para implantação na rede do Piloto Drex, a equipe do projeto analisou diversas opções de mercado voltadas para a questão da privacidade em redes DLT. Em todas as avaliações, foi considerada a capacidade das soluções tanto em atender aos requisitos de negócio definidos no item 3.1, quanto em avaliar a programabilidade das soluções com foco na privacidade dos dados, sendo este último o principal desafio do piloto. Com base nessas definições, optou-se por soluções que abrangem diferentes arquiteturas de privacidade e propostas de solução, utilizando ZKP e segregação de redes, conforme listado abaixo:

- **Anonymous Zether** – ZKP e baseado em contas (*account-based*);
- **Starlight** – ZKP e baseado em *tokens* (*token-based*);
- **Rayls** – ZKP com segregação de redes e movimentação de *tokens;*
- **Microsoft Nova ZKP** – ZKP com segregação de redes e *tokens.*

É importante destacar que as descrições e avaliações das soluções testadas foram baseadas nas versões implantadas para teste na rede Drex e conforme detalhado nas seções seguintes para cada solução. Evoluções ocorridas em fases posteriores não estão incluídas neste relatório e poderão ser avaliadas em futuras publicações.

Para todos os casos de uso incluídos no escopo do Piloto, conforme descrito na seção 1.5 , foram desenvolvidos contratos inteligentes inicialmente sem soluções de privacidade. Em seguida, novos contratos foram criados com adaptações específicas para testar cada solução de privacidade. O objetivo final era alcançar o DvP de TPF entre clientes de diferentes instituições, passando pela implementação de parte dos outros fluxos descritos.

3.3.1. Anonymous Zether

A solução Anonymous Zether, desenvolvida pelo JPMorgan e Consensys, baseia-se em um artigo científico da Universidade de Stanford em parceria com a Visa[5] . O artigo propõe um sistema para movimentação e gerenciamento privado de *tokens* ERC-20, utilizando criptografia de dados e ZKP. A solução implementada adiciona anonimato às transações, tornando-as não apenas privadas, mas também anônimas pela inviabilidade de identificação das partes envolvidas.

A criptografia utilizada no Anonymous Zether é assimétrica e homomórfica, permitindo realizar operações matemáticas diretamente sobre os dados criptografados. O algoritmo de cifra utilizado é o ElGamal.

O sistema utiliza um contrato blindado especializado, aqui referenciado como contrato Zether, que gerencia *tokens* a partir de ZKPs. Os *tokens* padrão ERC de um usuário são transferidos da carteira Ethereum na rede Besu para o contrato Zether, que cria representações privadas dos *tokens* e se torna o custodiante dos ativos transferidos. Assim, os *tokens* públicos armazenados em contratos ERC são convertidos em representações privadas no contrato Zether e, após a transferência, todas as movimentações são realizadas com chaves criptográficas especializadas do contrato Zether que ficam em posse do usuário e não possuem vínculo com as chaves privadas das contas Ethereum.

A criptografia dos dados garante o sigilo do conteúdo das transações, mas ainda permite a identificação da origem e do destino de uma operação. Para adicionar anonimato, foi criado o conceito de grupo de anonimidade. Em vez de apenas o pagador e o recebedor estarem envolvidos na transação, permitindo a identificação dos participantes reais, são adicionados outros participantes chamados "*decoys*". Esses *decoys* entram na transação com operações de valor zero, apenas para ocultar os verdadeiros envolvidos. Como os valores das operações são criptografados, torna-se inviável distinguir quem é pagador, o recebedor ou simplesmente um *decoy*.

5 BÜNZ, Benedikt; AGRAWAL, Shashank; ZAMANI, Mahdi; BONEH, Dan. *Zether – Towards Privacy in a Smart Contract World*. Disponível em: https://ia.cr/2019/191.

Toda transação de movimentação de ativos em um contrato Zether inclui a operação de débito e os créditos correspondentes, além de uma ZKP de que o pagador possui saldo suficiente para efetivar a operação e que o valor debitado é igual à soma dos valores creditados. Como a prova depende do saldo, é necessário garantir que este saldo não seja alterado entre o momento da criação da prova e o momento de sua validação, o que aconteceria se, por exemplo, o pagador recebesse um crédito durante este intervalo .

Para evitar essa situação, o protocolo Zether introduziu o conceito de "época" (epoch). Uma época é um período arbitrário, configurável por contrato Zether, vinculado ao número do bloco e utilizado na validação da prova. Durante uma época, os saldos permanecem congelados. Todas as transações enviadas durante a mesma época são armazenadas em uma lista de transações pendentes e, somente ao final da época, as provas são validadas e os saldos são atualizados com os valores das operações.

3.3.1.1. Fluxos implementados

No Piloto, foram implementados fluxos de transferência simples para Drex de Atacado e TPFt, além de um fluxo de troca atômica entre esses ativos. Utilizou-se a versão da solução criada a partir de repositório da Consensys[6].

Transferência Simples

Para a transferência simples, foi necessário criar um contrato Zether específico para cada ativo. Os participantes depositam seus Drex de Atacado ou TPFt no contrato Zether correspondente e realizam transações usando suas chaves El Gamal cadastradas para movimentação nesses contratos. O tempo da época para os fluxos de transferência simples foi configurado para seis segundos.

Troca Atômica

Para efetuar a troca atômica entre Drex de Atacado e TPFt, foi necessária a implementação de três contratos, buscando manter a anonimidade do protocolo:

- um contrato Zether para a transferência do Drex de Atacado;
- um contrato Zether para a transferência de TPFt;
- um contrato intermediário para efetuar a validação, o *match* da operação com as condições pré-acordadas e a troca atômica dos ativos.

6 Disponível em: https://github.com/kaleido-io/anonymous-zether-client/tree/real-digital. Acesso em: 22 dez. 2023.

A efetivação da troca segue o seguinte fluxo:

i. vendedor e comprador concordam com as chaves Ethereum que serão usadas na troca;
ii. cada parte gera a transação de transferência de seu respectivo ativo e submete ao contrato intermediário de troca. A transação é similar a uma transferência simples, informando os dados criptografados da operação e os *decoys* envolvidos. No entanto, em vez de submeter a prova para efetivar a operação, o participante envia apenas o *hash* da prova;
iii. o contrato de troca trava o *hash* da prova no contrato Zether do ativo correspondente, garantindo que somente o contrato de troca possa usá-la;
iv. o contrato de troca emite um evento, informando às partes sobre a submissão completa da operação;
v. as partes leem o evento e validam se a operação da contraparte corresponde ao que foi acordado;
vi. cada parte submete a ZKP específica da sua operação para efetivar a transferência;
vii. ao receber as duas ZKPs, o contrato de troca executa as transações de forma atômica, movendo os ativos nos respectivos contratos Zether.

É importante ressaltar que o fluxo envolve o envio de quatro transações pelas contrapartes, e todas devem ocorrer em uma única época, configurada para sessenta segundos. A época não se inicia com a primeira transação de troca; ela possui um tempo de início fixo, relacionado ao número atual do bloco na rede Besu.

3.3.1.2. Avaliação do BC

Após os testes realizados com a solução Anonymous Zether destacamos os seguintes pontos principais.

Privacidade

A versão avaliada da solução garante a privacidade e o anonimato das transações. No entanto, isso também oculta essas operações da autoridade sobre o *token*, que não consegue acompanhar as operações na rede, identificar as transferências efetuadas ou determinar em qual carteira o ativo se encontra.

Criptografia

Como as movimentações dentro dos contratos Zether só podem ser efetivadas com o uso de chaves criptográficas específicas, que ficariam sob a posse do agente de acesso do usuário, as autoridades sobre o *token* não teriam poder para executar

bloqueios parciais de saldos ou realizar movimentações em nome do cliente. Caso a chave seja perdida, o *token* não poderá mais ser movimentado e estará perdido.

É essencial que as autoridades tenham visibilidade e controle sobre o *token* para cumprir suas obrigações legais, regulamentares ou contratuais. Sem essa capacidade, as autoridades não conseguiriam monitorar atividades suspeitas, prevenir fraudes ou garantir a conformidade com as leis e os regulamentos aplicáveis, comprometendo a segurança e a integridade da Plataforma Drex.

Escalabilidade

Com o limite de envio de uma transação por época, a solução escala com o número de usuários ou com a distribuição do saldo por várias chaves de um mesmo usuário para permitir o envio de múltiplas transações. No entanto, essa abordagem dificulta a gestão de saldos ao se incluir a dimensão de escalabilidade.

Usabilidade e tempo de resposta

As épocas estabelecidas para um determinado negócio podem impor limitações devido à necessidade de sincronização entre as contrapartes e à alta taxa de falhas para períodos curtos, prejudicando a experiência do usuário e o tempo de resposta do sistema, o que pode afetar a satisfação dos usuários e comprometer a eficiência operacional do sistema.

Programabilidade

A programabilidade é limitada pelo conceito de época. Embora seja possível implementar casos de uso que envolvam promessas de pagamento condicionais, como trocas atômicas, é necessária a execução sincronizada das contrapartes. Um curto espaço de tempo resulta em um elevado número de falhas, enquanto um maior tempo de época reduz o número de possíveis transações. Quanto maior o número de ativos envolvidos no negócio, maior a dificuldade de sincronização das operações dentro de um período pré-estabelecido.

A execução de operações complexas de forma atômica pode resultar em falhas na coordenação de transações, aumento do risco de erros e dificuldades na integração de novos serviços.

3.3.1.3. Avaliação dos participantes

O BC, de forma complementar à avaliação própria, conduziu uma consulta para levantar a percepção dos participantes sobre os testes de privacidade utilizando a solução Anonymous Zether. De forma geral, os participantes destacaram como ponto

positivo a capacidade de realizar transações de forma anônima e privada, embora alguns tenham colocado a falta de visibilidade pela autoridade sobre o *token* como um grande problema em relação à questão da privacidade.

Os pontos de atenção mais citados foram questões em torno do conceito de época, que trouxe várias consequências negativas na percepção dos participantes. Entre essas consequências, destacaram-se a dificuldade em escalar o número de transações às necessidades da Plataforma Drex e a complexidade de uso devido à necessidade de execução de vários passos dentro de uma época, resultando em um alto número de falhas. A configuração do tamanho da época e a dificuldade de equacionamento dos pontos acima foi evidenciado de forma relevante nas contribuições: um menor tempo de época permitiria um maior número de transações, em contraponto, há necessidade de execução sincronizada das contrapartes em um curto espaço de tempo, o que acaba gerando maior número de erros.

3.3.2. Rayls

A Rayls, desenvolvida pela Parfin, é uma solução que visa adicionar privacidade a uma rede DLT permissionada, criando *ledgers* segregados baseados em EVM. Esses *ledgers* são interoperáveis através de uma camada subjacente comum de comunicação. Dessa forma, os *tokens* necessários para a execução de um contrato no *ledger* segregado são transferidos e depositados no próprio *ledger*, garantindo que apenas o dono do *ledger* tenha visibilidade das operações realizadas.

A arquitetura dessa solução é composta por três componentes principais:

- ***Privacy Ledger* (PL)** – *ledger* privado de um participante, com identificação única na rede, onde todos os seus ativos são armazenados. Baseado em EVM, permite a execução de contratos inteligentes com total privacidade;
- ***Commit Chain*** – rede DLT que atua como camada subjacente entre os PLs. É utilizada para comunicação entre os *ledgers* e para garantir a consistência dos saldos dos ativos;
- ***Privacy Bridge*** – conjunto de contratos inteligentes e um componente chamado *relayer* que realizam a movimentação dos ativos de forma privada entre os *ledgers* e sincronizam os ativos transferidos. Baseado no padrão ERC-5164, o protocolo visa assegurar a consistência das transações entre *ledgers*.

Esses três componentes formam uma *subnet*. A proposta da solução é que diferentes *subnets*, segregadas por área de atuação, possam também ser interconectadas.

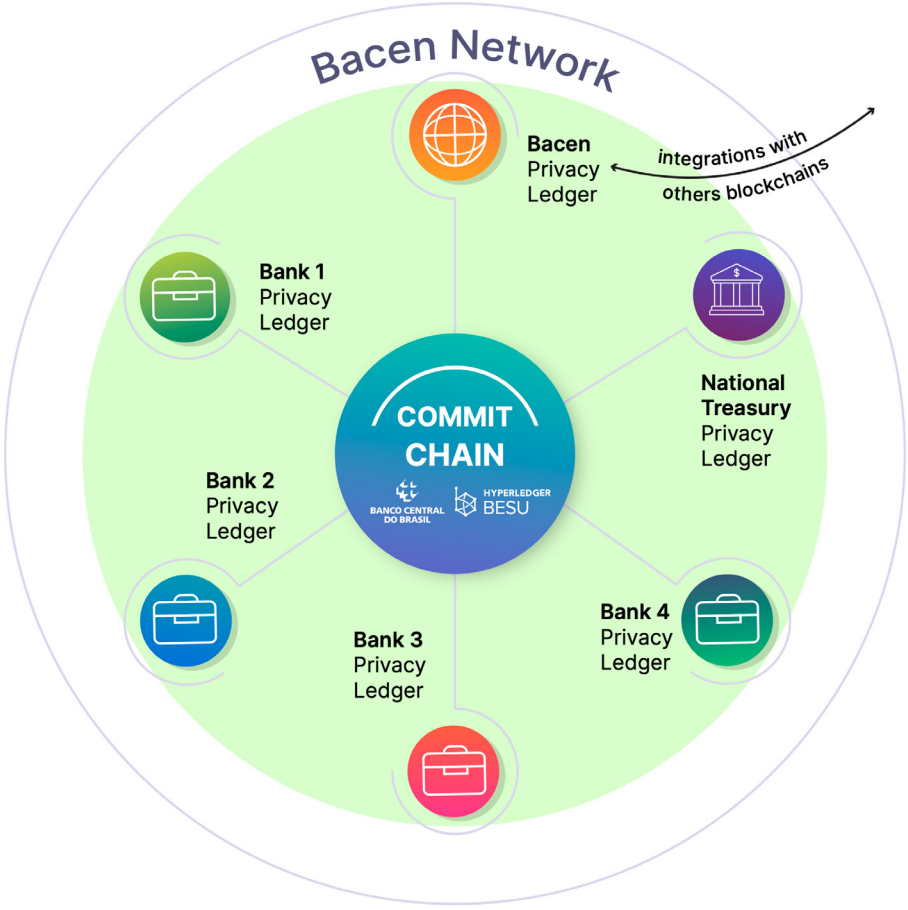

Figura 5

No contexto do piloto, foi criada a subnet do Drex, onde o BC, o Selic e cada um dos participantes possuem sua própria PL. A camada compartilhada de comunicação é a própria Plataforma Drex implantada para o piloto.

Nesse cenário de *ledgers* segregadas, os ativos depositados em cada PL são representados por contratos inteligentes padrão ERC, sem a necessidade de criptografia para ocultar saldos, já que apenas o proprietário da PL tem acesso às informações. A PL do emissor do ativo possui o contrato original e registra o *bytecode* desse contrato na *commit chain*. A partir do *bytecode*, a solução replica o contrato original do ativo em todas as outras PLs que compõem a subnet. Esse mecanismo impede que um participante faça uma emissão indevida de um ativo na sua própria PL e o transmita indevidamente a outro participante.

No contrato inteligente dos ativos que podem ser movimentados entre as diversas PLs, além dos métodos padrão ERC, há um método denominado “teleporte atômico”, responsável pela movimentação dos ativos. Sempre que um ativo precisar ser

transferido entre *ledgers*, o ativo na PL origem é queimado e, em seguida, o teleporte será executado. Em linhas gerais, o teleporte, com o auxílio de um componente denominado *relayer,* executa um conjunto de operações que orquestram a solicitação para emissão do ativo na PL de destino e a confirmação da operação na *commit chain*, ou a execução de transações compensatórias, como a solicitação para reemissão do ativo na PL original, em caso de falha ou *timeout* do lado recebedor.

Visão simplificada do Teleport na Rayls

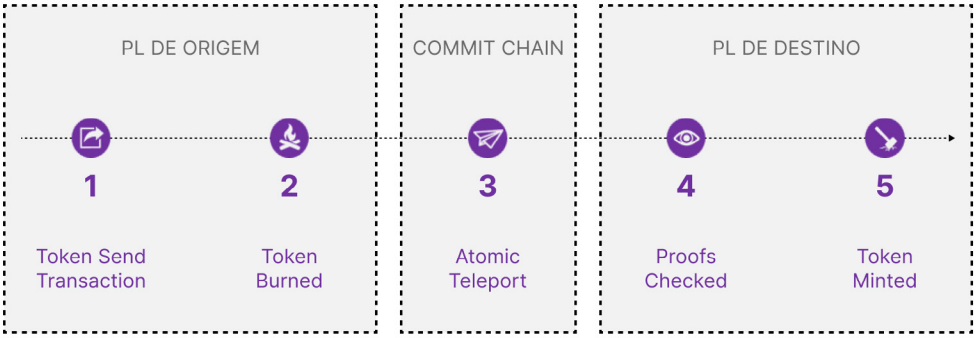

Figura 6

O Drex de Atacado é originalmente emitido na PL do BC e o TPFt na PL do Selic. Ambos os ativos podem ser transferidos entre PLs distintas utilizando o método de teleporte e com registro na *commit chain*. Por outro lado, o Drex de Varejo, sendo o *token* de uma classe de ativo cuja autoridade são as instituições participantes do piloto, é emitido por cada participante em sua própria PL. Devido a restrições de negócio, o Drex de Varejo não pode ser transferido entre instituições, ficando restrito à PL de cada instituição e, nesse caso, como não há movimentação entre *ledgers*, o ativo não é registrado na *commit chain* para controle de emissão em *ledgers* distintas.

Todos os ativos que podem ser movimentados entre PLs são registrados na *commit chain*. Cada PL registra periodicamente e de forma criptografada o saldo mais recente do ativo depositado em sua PL. A criptografia utilizada permite validar se a soma dos saldos de cada PL corresponde ao total emitido na PL original pelo agente emissor do ativo. Esses registros permitem a realização de uma auditoria externa de forma assíncrona, verificando inconsistências e gastos duplos. Na solução avaliada, foi implementado um sistema de verificação automatizado chamado Flagger, que sinaliza inconsistências após a execução de transações que desrespeitam as regras do sistema.

3.3.2.1. Fluxos implementados

Com a solução Rayls, foi possível implementar fluxos de transferência de todos os ativos, além da compra e venda de TPFt, tanto com Drex de Atacado quanto com Drex

de Varejo. Todos os casos de uso foram implementados pela Parfin e validados pela equipe do projeto para avaliação e entendimento do funcionamento da solução.

Para a implementação dos fluxos, foi utilizada a versão 1.8.6[7], que faz uso do protocolo *Rayls Atomic Teleport* para criptografar informações das transações na *commit chain* e permitir a validação das provas e das consistências pelo auditor externo. Evoluções e novos protocolos implementados pela Rayls não foram avaliados no escopo da primeira fase.

Transferência de Drex de Atacado e TPFt

O fluxo de transferência de Drex de Atacado, TPFt ou qualquer outro ativo que, conforme especificação, podem ser transportados entre PL segue o seguinte processo:

i. o ativo é queimado na PL original;
ii. o processo de teleporte é iniciado e solicita à PL de destino a emissão do ativo com base em evidências da execução do *burn* na *commit chain;*
iii. a PL de destino verifica as evidências apresentadas na *commit chain*. Se tudo estiver correto, o ativo é emitido na PL de destino;
iv. a operação é confirmada na *commit chain.*

Transferência de Drex de Varejo

Para a transferência de Drex de Varejo, foram implementados dois fluxos distintos, dependendo das contrapartes envolvidas no pagamento.

Quando o pagador e o recebedor são clientes da mesma instituição, a transferência é simples, seguindo o padrão ERC-20 dentro da mesma PL.

Entretanto, quando as contrapartes são clientes de instituições distintas, o pagamento com Drex de Varejo envolve também uma transferência de Drex de Atacado entre os participantes das PLs envolvidas, conforme especificado pelo fluxo de negócio. Os passos implementados na solução são:

i. O Drex de Varejo do pagador é queimado na PL de origem;
ii. O Drex de Atacado da instituição pagadora é queimado na PL de origem;
iii. O processo de teleporte é iniciado e solicita à PL de destino a emissão de Drex de Atacado para o participante recebedor e Drex de Varejo para o cliente com base em evidências da execução do *burn* na *Commit Chain;*

7 A versão utilizada estava disponível em https://github.com/raylsnetwork/piloto_rd em 12 de agosto de 2024.

iv. A PL de destino verifica as evidências apresentadas na *commit chain*. Se tudo estiver correto, o Drex de Atacado e o Drex de Varejo são transferidos e emitidos na PL de destino;
v. A operação é confirmada na *commit chain*.

Troca atômica

Foram implementados fluxos de troca atômica entre Drex de Atacado e TPFt e também entre Drex de Varejo e TPFt.

Em ambas as trocas, o fluxo implementado exige que os ativos sejam transferidos para a PL do Selic seguindo os fluxos de transferência já exemplificados. Nessa PL realiza-se a troca entre os participantes envolvidos e, após a troca, cada participante é responsável por recuperar o ativo na PL da troca e o transportar para sua própria PL.

3.3.2.2. Avaliação do BC

Após os testes realizados com a solução Rayls destacamos os seguintes pontos principais.

Privacidade das Operações

A versão avaliada da solução garante a privacidade e o anonimato das transações. No entanto, após a emissão do ativo e sua transferência para a PL de um participante, não foi implementado nesta versão um controle que permita às autoridades sobre o *token* acompanhar as transferências, identificar as carteiras de localização dos *tokens*, efetuar movimentações ou executar bloqueios totais ou parciais de saldo, se necessário.

É essencial que as autoridades tenham visibilidade e controle sobre o *token* para cumprir suas obrigações legais, regulamentares ou contratuais. Sem essa capacidade, as autoridades não conseguiriam monitorar atividades suspeitas, prevenir fraudes ou garantir a conformidade com as leis e regulamentos aplicáveis, comprometendo a segurança e a integridade da Plataforma Drex.

Validação assíncrona

Na versão testada com o protocolo *Rayls Atomic Teleport*, as informações são criptografadas na *commit chain* e a validação de provas e consistências é executada de forma assíncrona por um auditor externo (Rayls Flagger). Possíveis irregularidades são apontadas apenas após a execução das transações, e isso pode permitir que transações fraudulentas sejam confirmadas na PL e detectadas apenas posteriormente pelo auditor externo, apresentando desafios significativos para a governança do sistema, pois transações confirmadas podem ser consideradas inválidas posteriormente por desrespeitarem regras do sistema, como o gasto duplo de um ativo em uma PL.

Escalabilidade

A arquitetura de segregação de redes apresentada pela Rayls, com a movimentação de ativos para as *ledgers* privadas, oferece um ganho de escala quando os ativos transacionados já estão depositados na *ledger* e não têm a necessidade de serem transferidos entre os participantes com transferência pela *commit chain*. No entanto, para operações entre participantes distintos que demandam a movimentação de ativos, houve um aumento no tempo de execução devido à necessidade de realizar operações entre PLs distintas, além dos registros e das operações de sincronização na camada de comunicação.

Tempo de resposta

Durante os testes, observou-se que a emissão de um Drex de Atacado e transferências simples de *tokens* entre PLs levaram de 10 a 60 segundos, enquanto operações mais complexas, como DVP de Drex de Varejo e TPFt, variaram de 1 a 4 minutos.

O tempo de resposta pode afetar a satisfação dos usuários e comprometer a eficiência operacional do sistema. Entretanto, apesar dos números aferidos, cabe destacar que a escalabilidade e a melhoria do tempo de resposta das transações não foram objeto de avaliação, e a evolução de desempenho também não foi trabalhada, pois não estavam no escopo desta fase do piloto.

Programabilidade

A arquitetura proposta apresenta desafios relacionados à programabilidade de ativos em *ledgers* distintos. Com o protocolo *Rayls Atomic Teleport*, para interoperar ativos, foi necessário implementar estratégias comuns à integração de sistemas centralizados, como *retry*, *timeout* e transações compensatórias em caso de falha. Uma eventual falha nesses protocolos pode fazer com que, por exemplo, parte do processo não seja executado e um participante perca o saldo envolvido na operação.

A componibilidade de serviços também foi prejudicada pela segregação dos ativos em *ledgers* distintas. Tendo em vista que, para contemplar a privacidade, uma *ledger* não visualiza ativos de outra, os serviços compostos precisam movimentar os ativos envolvidos para uma *ledger* específica do negócio tratado. Para cada novo serviço, pode ser necessária a criação de uma nova *ledger* para sua execução.

A execução de operações complexas de forma atômica pode resultar em falhas na coordenação de transações, aumento do risco de erros e dificuldades na integração de novos serviços.

3.3.2.3. Avaliação dos participantes

O BC, de forma complementar à sua própria avaliação, conduziu uma consulta para levantar a percepção dos participantes sobre os testes de privacidade utilizando a solução Rayls. Os principais pontos positivos destacados na avaliação dos participantes foram a interoperabilidade com outras EVMs e a arquitetura para garantir a privacidade, por meio do processamento privado no PL de cada instituição, não sendo possível visualizar os dados das transações na camada subjacente de comunicação e nem na *ledgers* privadas dos outros participantes.

Por outro lado, os pontos de atenção, segundo os participantes, também foram indicados em torno da complexidade da arquitetura da solução e da infraestrutura necessária. Eles destacaram a complexidade da arquitetura, da infraestrutura necessária e a dificuldade na identificação de erros. Outro ponto mencionado foi a forte dependência do componente *relayer* para comunicação entre PLs.

3.3.3. Starlight

O Starlight, solução de privacidade e anonimato desenvolvida pela Ernst & Young (EY), visa facilitar a criação de aplicações de privacidade para DLTs baseados no padrão EVM. Essa solução busca simplificar o uso de ZKP em contratos inteligentes, permitindo que os desenvolvedores se concentrem na lógica do contrato sem a necessidade de lidar com a complexidade dos circuitos criptográficos.

Para isso, o Starlight introduz uma linguagem de domínio específico chamada Zolidity, que estende a programação Solidity com funções específicas de privacidade. Com Zolidity, é possível marcar saldos de contratos ERC-20 como privados e realizar transações de forma sigilosa.

Para garantir a privacidade e segurança das transações, a solução baseia-se em *commitments*[8], que representam transações não gastas, conforme o modelo *unspent transaction output* (UTXO)[9]. Para cada ativo padrão ERC-20 transferido da carteira Ethereum na rede Besu para o contrato privado Starlight, é criado um novo *commitment*, que se torna a representação privada do *token* transferido. Para cada nova movimentação envolvendo os *tokens* privados, são gerados novos *commitments* e o *commitment* que originou a transação é marcado como gasto, impedindo a sua reutilização.

8 *Commitment* é um conceito criptográfico que permite que um agente se comprometa com um valor específico sem a necessidade de revelar este valor e sem a possibilidade de alterá-lo após a criação do compromisso.

9 UTXO é um modelo utilizado em criptomoedas como Bitcoin. Representa a quantidade da moeda que permanece não utilizada após uma transação. Cada transação envolve entradas e saídas, e os UTXOs são os saldos disponíveis que um usuário pode gastar.

A privacidade das operações é garantida porque cada *commitment* é formado pelo *hash* das informações da operação, como endereço de origem, destino, valor e outros dados necessários para a operação. O *hash* é visível a todos com acesso à rede, mas os campos que o geraram (pré-imagem) são criptografados e conhecidos apenas pelo dono do *commitment*.

As chaves criptográficas utilizadas no contrato privado Starlight, que ficam em posse do agente de acesso do usuário, não têm vínculo com as chaves privadas das contas Ethereum.

Para garantir a integridade e autenticidade dos valores transacionados, cada *commitment* gerado é registrado em uma árvore de *hash* (árvore de Merkle).

Os componentes necessários para a utilização dos contratos privados Starlight são obtidos por meio de um processo de transpilação fornecido pela própria solução. Esse processo, a partir do contrato inteligente em Zolidity, gera um Zolidity Application (Zapp) composto pelos contratos privados que serão implantados na rede DLT, bem como toda a infraestrutura *off-chain* necessária para a interação com esses contratos, conforme descrito abaixo:

- **contratos privados** – contratos Solidity que definem as regras de negócio, armazenam os *commitments* e validam as provas de conhecimento zero;
- **orquestrador** – aplicação de cliente que disponibiliza APIs para interação com os contratos e coordena a chamada aos outros componentes da infraestrutura;
- **Zokrates-worker** – gerador das ZPKs;
- **Timber** – componente responsável pelo armazenamento *off-chain* de toda a árvore de *commitments* e pela sincronização com a rede. A arquitetura da solução, para reduzir os custos da transação, armazena a árvore de Merkle de forma parcial nos contratos privados da rede e de forma completa na parte cliente da solução, sendo necessária a sincronização pelo Timber sempre que um novo *commitment* é registrado.

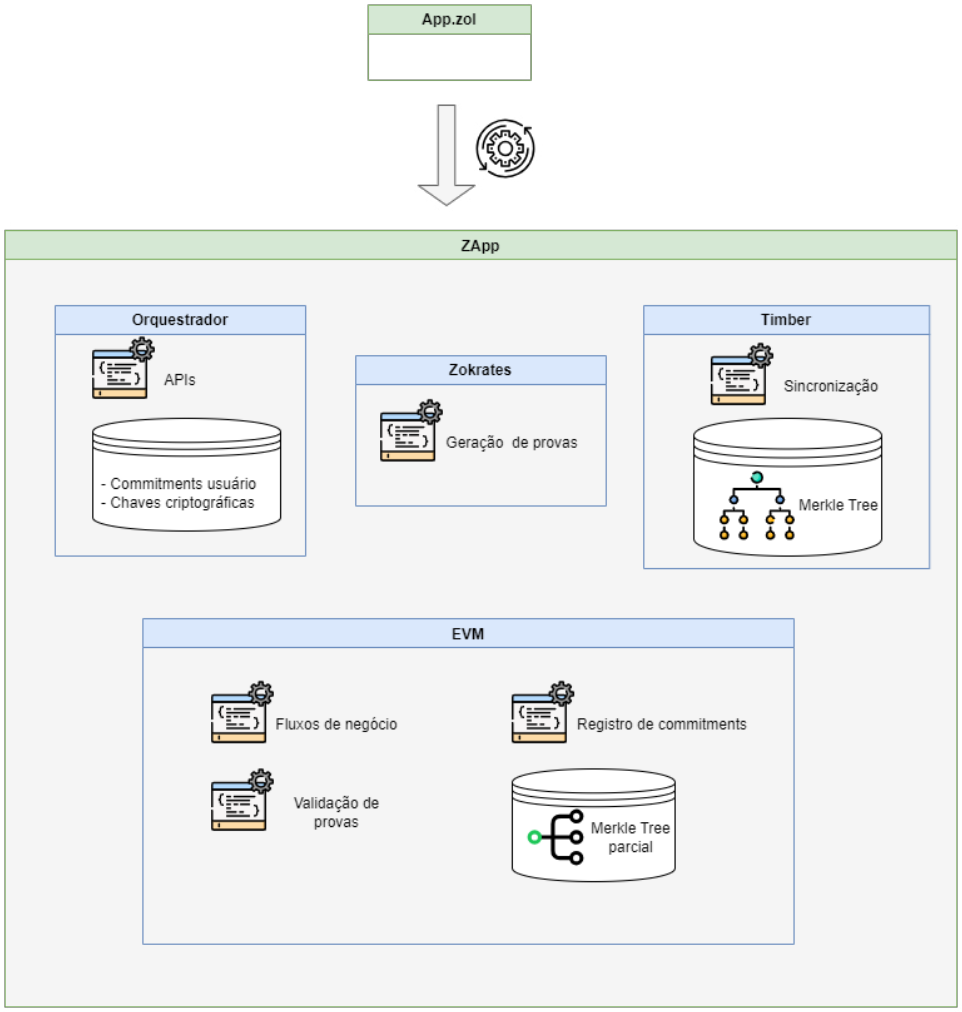

Figura 7

3.3.3.1. Fluxos implementados

No piloto, foram implementados fluxos de transferência simples para Drex de Atacado e TPFt, além de um fluxo de troca atômica entre esses ativos.

Transferência simples

Para o cenário de transferência do Drex de Atacado, foi desenvolvido um contrato Zolidity, baseado no exemplo *Escrow*, disponível no repositório da solução[10].

Uma transferência simples na solução Starlight segue o modelo UTXO, em que uma ou mais transações são "gastas" e uma ou mais transações de saída são geradas. Para realizar a transferência, o contrato inteligente é acionado pelo pagador através do Zapp e recebe os seguintes parâmetros:

10 A solução adaptada e implantada foi disponibilizada em 2 de abril de 2024 e pode ser encontrada em https://github.com/kaleido-io/starlight/tree/refactor.

- **lista de *nullifiers*** – indica quais *commitments* estão sendo gastos;
- **lista de novos *commitments*** – gera-se um *commitment* de pagamento para o recebedor e, se houver valor restante, gera-se um outro *commitment* para o pagador correspondente à diferença entre o valor original e o valor pago;
- **pré-imagem dos *commitments* gerados** – dados da transação criptografados com a chave pública do recebedor do *commitment*;
- **ZKP** – garante a validade da transação.

O contrato inteligente valida a ZKP e emite eventos para atualizar a árvore de Merkle e registrar o novo *commitment*. O recebedor da transferência deve então ler esses eventos, usar sua chave privada para obter a pré-imagem do *commitment* recebido, obter a nova raiz da árvore de Merkle e atualizar sua árvore local.

Troca Atômica

O fluxo de troca atômica de TPFt por Drex de Atacado, envolvendo dois participantes, foi implementado pela EY em uma aplicação chamada SwapEscrow[11].

As trocas (*swaps*) ocorrem em duas etapas e podem ser iniciadas tanto pelo vendedor quanto pelo comprador do título, seguindo os passos abaixo.

Etapa 1 – Proposta de Troca

i. O proponente faz a proposta de troca, criando um *commitment* com os dados pré-acordados da operação e gasta seu ativo como confirmação da transação.
ii. Após enviar a proposta, é gerada uma identidade (ID) de troca única (*Swap ID*), que é enviada à contraparte junto com a pré-imagem do *commitment* de troca criptografada com uma chave conhecida por ambas as partes.

Etapa 2 – Conclusão da Troca

i. A contraparte recebe a *Swap ID* gerada na primeira etapa e valida as informações da proposta de troca.
ii. A contraparte confirma a operação informando a *Swap ID* gerada e gastando seu ativo como confirmação da operação. Com isso, a troca atômica é efetuada, transferindo o Drex de Atacado ao vendedor e o TPFt ao comprador e permitindo que os participantes incorporem os respectivos *commitments* em seus bancos de dados.

11 Disponível em https://github.com/eybrativosdigitais/zapp-swapescrow-drex. Acesso em: 5 jul. 2024.

Importante destacar que, enquanto a contraparte não efetivar sua operação, a operação pode ser cancelada e o ativo colocado em garantia resgatado pelo proponente.

3.3.3.2. Avaliação do BC

Após os testes realizados com a solução Starlight, destacamos os seguintes pontos principais.

Privacidade das operações

A versão avaliada da solução garante a privacidade e o anonimato das transações. No entanto, isso também oculta essas operações das autoridades sobre o *token* , que não conseguem acompanhar as operações na rede, identificar as transferências efetuadas ou determinar em qual carteira o ativo se encontra.

Criptografia

Como as movimentações dentro dos contratos privados só podem ser efetivadas com o uso de chaves criptográficas específicas, que estão sob a posse do agente de acesso do usuário, as autoridades sobre o *token* não têm poder para executar bloqueios parciais de saldos ou realizar movimentações em nome do participante. Caso a chave seja perdida, o ativo não poderá mais ser movimentado e estará perdido.

É essencial que as autoridades tenham visibilidade e controle sobre o *token* para cumprir suas obrigações legais, regulamentares ou contratuais. Sem essa capacidade, as autoridades não conseguiriam monitorar atividades suspeitas, prevenir fraudes ou garantir a conformidade com as leis e regulamentos aplicáveis, comprometendo a segurança e a integridade da Plataforma Drex.

Programabilidade

A programabilidade da solução depende da capacidade da linguagem Zolidity em suportar as características do negócio. O suporte ao DvP com dois ativos foi criado pela EY ao longo do piloto, permitindo a implementação da troca atômica de Drex de Atacado e TPFt. No entanto, o DvP do cliente, que envolve três ativos, não pode ser implementado, pois ainda não é suportado pela linguagem.

A solução desenvolvida pela EY implementa todos os *tokens* e casos de uso em um único contrato inteligente. Essa escolha de projeto resulta em um problema de falta de componibilidade, pois a introdução de um novo tipo de ativo exige a reconstrução completa da solução desde o início.

Escalabilidade e tempo de resposta

A solução permite a execução de múltiplas transações simultâneas por participante, o que possibilita a escalabilidade. No entanto, o tempo médio observado para a execução de cada transação é de 15 a 20 segundos.

O tempo de resposta pode afetar a satisfação dos usuários e comprometer a eficiência operacional do sistema. Entretanto, apesar dos números aferidos, cabe destacar que a escalabilidade e a melhoria do tempo de resposta das transações não foram objeto de avaliação, e a evolução de desempenho também não foi trabalhada, pois não estavam no escopo desta fase do piloto.

Dados *off-chain*

O Starlight mantém dados privados *off-chain*. Esse *design* requer estruturas de dados resilientes fora da rede DLT, que devem ser mantidas de forma semelhante a um banco de dados em sistemas transacionais e centralizados. Falhas na sincronização entre as estruturas *off-chain* e o sistema impedem o participante de operar, trazendo riscos relevantes para a continuidade e confiabilidade das operações.

3.3.3.3. Avaliação dos participantes

O BC, de forma complementar à avaliação própria, conduziu uma consulta para levantar a percepção dos participantes sobre os testes de privacidade utilizando a solução Starlight. De maneira geral, os participantes destacaram a capacidade de realizar transações de forma anônima e privada, além da simplificação da interação com os contratos por meio do componente Zapp. Também foi mencionada, com relevância, a possibilidade de usar privacidade com pequenas alterações no código do contrato inteligente através do uso do transpilador.

O principal ponto de atenção foi a característica da solução de trabalhar com dados *off-chain* e a necessidade de sincronismo com a rede, o que traz riscos na percepção dos participantes. Houve relatos de falhas e quebras do sincronismo e consistência das informações. Outros pontos destacados foram: a criticidade, a complexidade e a necessidade de cada participante monitorar a sua infraestrutura responsável pelo armazenamento *off-chain*; a instabilidade e as falhas de conectividade entre os componentes.

3.3.4. Microsoft Nova ZKP

A solução Microsoft Nova ZKP apresenta uma abordagem distinta das outras soluções testadas, com uma arquitetura de segregação de ativos em camadas distintas e sem movimentação de *tokens*.

A avaliação da solução foi anunciada ao mercado em maio como uma solução adicional a ser testada no âmbito do piloto. Até a conclusão da fase I do piloto, em 7 de outubro de 2024, não foi possível avaliar os fluxos propostos nem realizar os testes com os participantes, deixando a solução fora do escopo de avaliação desta fase.

4 Segurança

Um dos principais riscos cibernéticos a serem endereçados em uma solução CDBC é a possibilidade de fraudes que exploram vulnerabilidades em contratos inteligentes. Uma falha no programa do contrato inteligente é caracterizada pela possibilidade de execução fora do comportamento desejado pelo programador e especificado pelas regras de negócio. Um exemplo emblemático foi o ataque à Decentralized Autonomous Organization (DAO)[12], com o roubo de milhões de dólares, que resultou em um *hard fork* do Ethereum.

Um ataque bem-sucedido pode causar negação de serviço em um contrato (impedindo sua utilização e o acesso aos *tokens* gerenciados por ele), ou a transferência indevida de moedas para a carteira do atacante.

As características de imutabilidade, descentralização e visibilidade dos contratos inteligentes aumentam o risco de falhas no código. Além disso, quanto maior o nível de programabilidade, maior a complexidade das ações que cada contrato precisa executar, e consequentemente maior a superfície de ataque.

A plataforma pública do Ethereum já tem documentadas dezenas de vulnerabilidades, que podem ser divididas em três categorias principais: Solidity, EVM e *blockchain*[13]. As redes permissionadas, tanto baseadas no Ethereum quanto as demais, estão suscetíveis a um subconjunto dessas vulnerabilidades, além de outras específicas de cada plataforma e linguagem de programação.

12 Disponível em: https://www.gemini.com/pt-br/cryptopedia/the-dao-hack-makerdao.

13 Disponível em: https://link.springer.com/chapter/10.1007/978-3-662-54455-6_8.

Devido a sua popularidade, diversas ferramentas de análise foram desenvolvidas para detectar as vulnerabilidades em contratos inteligentes no padrão EVM antes que o contrato seja implantado na rede. Essas ferramentas, de forma geral, podem ser aproveitadas nos contratos das redes permissionadas baseadas no Ethereum.

Na primeira fase do Piloto Drex, foram utilizadas duas ferramentas de análise para detectar potenciais vulnerabilidades nos códigos dos contratos inteligentes desenvolvidos:

- **Slither**[14] **–** ferramenta que analisa o código dos contratos de forma estática em busca de diversas vulnerabilidades conhecidas;
- **Mythril**[15] **–** ferramenta de análise dinâmica, que executa o código em uma EVM e dispara diversas transações com o objetivo de identificar respostas inadequadas do programa que poderiam ser exploradas.

A execução dessas ferramentas permitiu que eventuais vulnerabilidades fossem corrigidas antes da implantação dos contratos na rede DLT. No entanto, cabe ressaltar que o uso de ferramentas automatizadas não é suficiente para detectar todas as potenciais vulnerabilidades em códigos de contratos inteligentes. Uma verificação manual complementar realizada por especialistas em segurança de contratos inteligentes é indicada para viabilizar o uso de uma solução CBDC em produção.

4.1. Testes/serviços futuros necessários

Além de complementar a avaliação dos contratos inteligentes com revisões manuais realizadas por especialistas, foram identificados outros dois serviços de cibersegurança a serem executados no ambiente do Drex ainda na fase piloto.

4.2. Modelagem de ameaças

Recomenda-se a execução de uma avaliação baseada em modelagem de ameaças para identificar as principais ameaças cibernéticas e as respectivas ações mitigadoras a serem implementadas para viabilizar a implantação do Drex em produção.

Essa avaliação poderá mensurar os riscos cibernéticos que impactarão o Drex, em diversas dimensões, como:

14 Disponível em: https://github.com/crytic/slither.

15 Disponível em: https://github.com/Consensys/mythril.

- acessos não autorizados à rede;
- vazamento de dados;
- roubo ou perda de chaves privadas;
- quebra de criptografia; e
- fraudes em contratos inteligentes.

Para cada risco considerado inaceitável, a avaliação deve ter como resultado recomendações de ações que possibilitem a mitigação ou eliminação do risco.

4.3. Teste de intrusão

Recomenda-se a execução de um teste de intrusão (*pen testing*) para identificar possíveis brechas que um atacante poderia explorar e indicar ações de correção. Os profissionais responsáveis pelo teste de intrusão devem ter conhecimento especializado em redes DLT e buscar o comprometimento de nós, validadores, contratos inteligentes, chaves privadas, dados sigilosos, entre outros. Outro objetivo é explorar a segurança do permissionamento da rede, visando impedir e detectar acesso de nós não autorizados que possam causar o vazamento de informações ou a execução de transações de forma indevida.

O resultado do teste deve apresentar as vulnerabilidades e brechas existentes, bem como recomendações de ações corretivas para proteção do ambiente.

5 Itens não tratados e recomendações para os próximos passos

Para desenvolver uma plataforma completa que atenda aos requisitos de uma infraestrutura crítica do SFN, é essencial considerar diversos outros aspectos que não foram avaliados ou discutidos no âmbito desta fase do piloto. Entre os pontos considerados importantes para discussões futuras, os que merecem maior destaque são detalhados a seguir.

5.1. Escalabilidade

A Plataforma Drex tem como um dos objetivos disponibilizar um sistema descentralizado multiativos, onde novas funcionalidades possam ser oferecidas e combinadas na criação de serviços distintos. Portanto, sua escalabilidade e seu desempenho são fundamentais.

Os testes de desempenho realizados no âmbito do piloto foram conduzidos apenas para conhecer a capacidade da rede e avaliar os impactos de alterações relevantes no ambiente do piloto. Em um cenário de produção, a capacidade deve ser determinada com base nos requisitos dos serviços disponibilizados e na arquitetura da rede. Além disso, é necessário planejar como aumentar a capacidade ao longo do tempo e o que fazer ao se atingir o limite, uma vez que a arquitetura de *ledgers* distribuídas tem capacidade limitada, mesmo com o aumento de recursos computacionais.

5.2. Governança

Em uma plataforma descentralizada, a governança da rede deve ser bem estruturada, com validadores distribuídos entre as autoridades sobre os diversos *tokens*. É importante definir claramente quem pode criar e implantar contratos, além de quem se responsabiliza pelo seu funcionamento. Questões sobre remuneração dos serviços precisam ser abordadas. A relação entre programabilidade de serviços, responsabilização e remuneração deve ser cuidadosamente gerida para lidar com alterações internas nos serviços. Além disso, questões de propriedade intelectual, como a possibilidade de copiar contratos, também precisam ser discutidas.

5.3. Segurança

A segurança é um pilar central. Com os *ledgers* distribuídos, o vazamento de dados *on-chain* compromete toda a rede, afetando todos os usuários simultaneamente. Dado que contratos podem ser criados por diversos participantes e que serviços podem ser compostos, surge a questão: como mitigar falhas nos contratos que possam levar à execução inadequada ou ao roubo de ativos das carteiras dos usuários?

Além disso, para garantir a privacidade, é crucial validar a eficácia e a segurança dos algoritmos criptográficos utilizados. Também é fundamental avaliar os riscos de cibersegurança no ecossistema e implementar medidas de mitigação adequadas.

5.4. Integrações

As integrações da Plataforma Drex com outras plataformas e sistemas legados são essenciais para atender aos requisitos de negócio. Ao avaliar a possibilidade de integrações, é necessário ampliar as discussões relacionadas a:

- **padronização e protocolos** – garantir a compatibilidade entre diversos sistemas e plataformas;
- **escalabilidade** – assegurar que a integração suporte volumes adequados de transações;
- **análise de segurança e resiliência** – avaliar as vulnerabilidades que possam ser exploradas e a resiliência da infraestrutura de integração de modo a evitar a perda de ativos em caso de incidentes cibernéticos ou falhas operacionais;
- **conformidade regulamentar** – garantir que as integrações estejam em conformidade com as regulamentações locais e internacionais para a transferência de ativos entre redes distintas.

5.5. Infraestrutura

A infraestrutura deve ser resiliente e compatível com um serviço disponível em tempo integral, garantindo atualizações e correções contínuas da plataforma para manter sua robustez e confiabilidade.

5.6. Evoluções

Estudos sobre a evolução da Plataforma Drex devem incluir a possibilidade de migração de dados e de sistemas para outras plataformas, no caso, por exemplo, de descontinuidade na evolução da plataforma DLT adotada. Além disso, é importante considerar como atualizações e correções dos contratos inteligentes podem ser efetuadas, assegurando que a plataforma se mantenha atualizada e funcional.

5.7. Regulação

A tokenização pode levantar questões legais complexas. Em fases posteriores, é crucial abordar a legislação e a regulamentação da tokenização de ativos, que envolve ter um caminho claro para a criação, emissão e transferência de *tokens* na Plataforma Drex. Além disso, a validade jurídica de contratos inteligentes precisa ser estabelecida. Isso significa garantir que esses contratos, que são autoexecutáveis e baseados em código, sejam reconhecidos e aplicáveis nos tribunais e úteis na resolução de disputas.

A imutabilidade preconizada na Plataforma Drex assegura a integridade dos registros. No entanto, essa característica pode entrar em conflito com o direito ao esquecimento, um princípio na legislação de proteção de dados. Em fases futuras, é essencial desenvolver mecanismos que equilibrem a imutabilidade com a privacidade dos dados.

Nesse contexto, o BC conduz um projeto institucional voltado à identificação e à mitigação das inseguranças jurídicas, tanto no âmbito legal quanto infralegal, que envolvem a tokenização de ativos. Essa iniciativa busca consolidar um ambiente regulatório seguro e previsível, posicionando o Brasil como referência internacional no desenvolvimento desse modelo de negócio, cujo potencial de impacto econômico é significativo.

5.8. Negócio

Casos de usos adicionais devem ser avaliados, inclusive aqueles que preveem o uso de ativos não regulados pelo BC. Esse é um passo importante para explorar o potencial de inovação e eficiência que esses ativos podem trazer para o mercado financeiro.

A colaboração de inter-reguladores será essencial para criar um ambiente de teste abrangente e robusto, capaz de avaliar a viabilidade e a segurança de novos casos de uso em diferentes contextos regulatórios. Ao trabalhar em conjunto com diversos órgãos reguladores, poderemos assegurar que a Plataforma Drex seja adaptável e capaz de atender às necessidades de um mercado financeiro em constante evolução.

6 Conclusões

É provável que um grande esforço de adaptação seja necessário para que a Plataforma Drex possa servir como infraestrutura para serviços inovadores destinados à sociedade. Apesar de avanços importantes na direção da anonimização, as soluções testadas apresentam limitações que comprometem, no momento, sua adoção no contexto das necessidades de negócio estabelecidas. A falta de controle pelas autoridades sobre os *tokens* e as limitações na programabilidade e na componibilidade mostram que o estado das soluções carece de maturidade com relação aos requisitos essenciais para um sistema financeiro robusto e dinâmico.

Esses desafios destacam a necessidade de um desenvolvimento contínuo e de uma colaboração estreita entre reguladores, desenvolvedores, academia e participantes do mercado para superar as barreiras atuais. Somente através de um esforço conjunto será possível adaptar e evoluir as tecnologias para que possam atender plenamente às exigências de um sistema financeiro moderno e eficiente.

Essas constatações nos levaram a operacionalizar a fase II do piloto, que terá como escopo avançar nas questões de privacidade ao mesmo tempo em que abriremos para os participantes do piloto sugerirem seus casos de uso. Essa nova fase permitirá que exploremos casos de uso mais amplos, enquanto continuamos a abordar as preocupações com privacidade. Além disso, ao envolver os participantes na sugestão de casos de uso, esperamos identificar necessidades específicas e oportunidades de inovação que possam orientar o desenvolvimento contínuo da Plataforma Drex, tornando-a mais alinhada com as demandas reais do mercado e da sociedade.

Anexo I – Glossário

Agente de acesso
Participante do Drex responsável por apresentar os aplicativos ao usuário final, custodiar as chaves privadas dos usuários e protegê-los contra ataques cibernéticos.

Ativo
Conjunto composto por ativos financeiros, valores mobiliários, moedas e ativos do mundo real.

Atomicidade (processo atômico)
Processo composto onde todas as suas partes são ou concluídas de forma integral, sem falhas, ou todas são abortadas.

Autoridade
Entidade que possui credenciais conferidas por meios legais, regulamentares ou contratuais, permitindo-lhe priorizar comandos em relação às operações usuais de um *token*. No escopo desta fase do piloto, é o responsável por um ativo publicado na rede Drex.

Backdoor
Um método para contornar a autenticação ou outros controles de segurança em um sistema, frequentemente usado para acesso não autorizado.

Blockchain

Um livro-razão digital descentralizado e distribuído que registra transações em vários computadores de forma que os registros não possam ser alterados retroativamente sem a alteração de todos os blocos subsequentes e a conivência da rede.

Burn

O processo de remover permanentemente *tokens* de circulação.

Componibilidade

A capacidade de diferentes sistemas e componentes de *software* de se integrarem e funcionarem juntos de forma eficiente.

Cross-chain

A capacidade de diferentes *blockchains* de interagir e trocar informações ou ativos entre si.

Drex de Atacado

Vide introdução.

Drex de Varejo

Vide introdução.

Ethereum

Uma plataforma de *blockchain* descentralizada que permite a criação e execução de contratos inteligentes e aplicativos descentralizados (dApps).

Finality

A garantia de que uma transação não pode ser revertida ou alterada após ser confirmada.

Mint

O processo de criação de novos *tokens* em uma *blockchain*.

Off-chain

Transações ou dados que são processados fora da *blockchain* principal.

On-chain

Transações ou dados que são processados diretamente na *blockchain* principal.

Piloto Drex
Vide introdução.

Plataforma Drex
Vide introdução.

Programabilidade
A capacidade de uma plataforma de *blockchain* de suportar contratos que podem ser programados para executar automaticamente certas ações.

Projeto Drex
Vide introdução.

Participante
Entidade ou indivíduo que participa de uma plataforma.

Segmento Prudencial
Classifica instituições financeiras e conglomerados com base em seu porte, relevância internacional e perfil de risco. As categorias são S1, para instituições com ativos iguais ou superiores a 10% do PIB ou com atividade internacional relevante; S2, para ativos entre 1% e 10% do PIB; S3, para ativos entre 0,1% e 1% do PIB; S4, para ativos inferiores a 0,1% do PIB; e S5, para instituições não bancárias com perfil de risco simplificado e ativos inferiores a 0,1% do PIB.

Token
Vide explicação na introdução. Notar a diferença de significado para "*token-based*".

Token-based [controle da titularidade] baseado em *token*
É um mecanismo de controle de titularidade baseado na quantidade indivisível de um ativo e que deve ser transferido ou trocado em sua totalidade. Por exemplo, uma nota de 10 reais que não pode ser dividida ao meio para pagar uma conta de 5 reais é considerada *token-based*. É antagônico ao conceito de "conta", que é um mecanismo de controle de titularidade baseado no saldo divisível de um ativo. Por exemplo, o saldo de um cliente em reais no aplicativo do seu *home-banking*. Notar a diferença de significado para "*token*".

Anexo II – Acrônimos e abreviações

APIs
Interfaces de Programação de Aplicativos

BC
Banco Central do Brasil

BIS
Bank for International Settlements [Banco de Compensações Internacionais]

CBDC
Central Bank Digital Currency (Moedas Digitais de Banco Central)

CEG
Comitê Executivo Gestor do Piloto Drex

CL
Conta de Liquidação

CPU
Central Processing Unit (Unidade Central de Processamento)

DAO
Decentralized Autonomous Organization

DLT
Distributed Ledger Technology (Tecnologia de Registro Distribuído)

DvP
Delivery versus Payment (Entrega contra Pagamento)

DVt
tokens de Depósitos à Vista

EVM
Ethereum Virtual Machine

EY
Ernst & Young

I/O
Input/Output

JSON-RPC
JavaScript Object Notation-Remote Procedure Call

LBTR
Liquidação Bruta em Tempo Real

LFT
Letra Financeira do Tesouro

LTN
Letra do Tesouro Nacional

MEt
Moeda Eletrônica tokenizada

MPLS
Multiprotocol Label Switching

PL
Private Ledger ou *Privacy Ledger*

PvP

Payment versus Payment (Pagamento contra Pagamento)

QBFT

Quorum Byzantine Fault Tolerant

RSFN

Rede do Sistema Financeiro Nacional

RB

Reservas Bancárias

Selic

Sistema Especial de Liquidação e de Custódia

SMF

Sistema do Mercado Financeiro

SPB

Sistema de Pagamentos Brasileiro

SPI

Sistema de Pagamentos Instantâneos

STR

Sistema de Transferência de Reservas

STN

Secretaria do Tesouro Nacional

SFN

Sistema Financeiro Nacional

TCP

Transmission Control Protocol (Protocolo de Controle de Transmissão)

TEE

Trusted Execution Environment

TPF

Título Público Federal

TPFt

Título Público Federal tokenizado

TPS

Transações por Segundo

UDP

Protocolo de Datagrama de Usuário

UTXO

Unspent Transaction Output (Protocolo de Datagrama de Usuário)

ZKP

Zero-Knowledge Proof (Prova de Conhecimento Zero)

BANCO CENTRAL DO BRASIL