LIFT *papers*

REVISTA do LABORATÓRIO de INOVAÇÕES FINANCEIRAS e TECNOLÓGICAS

1ª EDIÇÃO

Fenasbac | BANCO CENTRAL DO BRASIL

LIFT Papers

Revista do Laboratório de Inovações Financeiras e Tecnológicas

Volume 1 • Número 1 • Março 2019

Ficha catalográfica elaborada pela Biblioteca do Banco Central do Brasil

LIFT Papers / Banco Central do Brasil. Vol. 1, n. 1, (março 2019). Brasília: Banco Central do Brasil, 2019.

Semestral
Disponível em:
https://www.liftlab.com.br/docs/lift_Red.pdf.
ISSN

1. Inovação Tecnológica – Brasil. 2. Sistema Financeiro – Brasil. 3. Crédito. I. Banco Central do Brasil.

CDU 336.7:004.738.5

O impacto da evolução tecnológica sobre o cotidiano também alcança a economia. As possibilidades que o mundo digital propicia não podem passar despercebidas a todos nós dedicados ao sistema financeiro do futuro. Para desenvolver esse potencial e conectar problemas com soluções, o Banco Central criou o LIFT, o Laboratório de Inovações Financeiras e Tecnológicas.

Com foco no sistema financeiro, o LIFT eleva mentes criativas do patamar da ideia à concretude. Empreendedores, pesquisadores e inventores que vislumbram novos caminhos tecnológico-financeiros encontram no LIFT a chance de lapidar suas ideias.

No laboratório, a inventividade do participante completa um tripé colaborativo com a experiência do BCB e o conhecimento de provedores de tecnologia. O resultado não poderia ser outro: transformar projetos em soluções e soluções em ganhos para a sociedade.

Esta revista compila os resultados da primeira edição do LIFT. Alguns projetos estão em fase avançada de implementação, outros vêm à tona aos poucos. O leitor especializado poderá conhecê-los mais a fundo enquanto o leitor meramente curioso terá uma noção do quanto suas finanças podem mudar, para melhor. Adicionalmente, a revista apresenta algumas reflexões sobre tendências na área.

Boa leitura.

Roberto Campos Neto

5 DLT para infraestrutura de pagamentos instantâneos

Pedro Prandini*
Marcelo Martins**
Eduardo Nuzzi***

Introdução: O Banco Central do Brasil (BCB) planeja implementar um ecossistema de pagamentos instantâneos. Para isso, estão sendo definidos tanto os requisitos fundamentais desse ecossistema como as ações necessárias para que o Sistema Financeiro Nacional (SFN) seja capaz de cumpri-los.
Problema: Não estão definidas as implementações tecnológicas necessárias para que o SFN proveja um ecossistema eficiente, seguro, competitivo e inclusivo.
Solução proposta: Foi desenvolvido um protótipo baseado em *Distributed Ledger Technology* (DLT) para desempenhar as funções de camada de liquidação e *switch*, centrais para o ecossistema. Foram realizados testes experimentais para investigar a adequação do protótipo aos requisitos fundamentais e foi feita uma demonstração prática com uma carteira digital.
Resultados: Os testes demonstraram que o protótipo processa transações em tempo menor do que o exigido pelos requisitos fundamentais e é capaz de processar um número de transações por segundo equivalente ao recorde do sistema de Transferência Eletrônica Disponível (TED). Além disso, o protótipo possibilita um modelo em que é possível tanto transações *peer-to-peer* como transações por meio de intermediários.
Conclusões: Em uma análise preliminar, o protótipo satisfaz demandas de rapidez e escalabilidade, possibilita um modelo de ecossistema inclusivo e competitivo, e permite a implementação de inovações além dos pagamentos instantâneos. Convém realizar experiências mais aprofundadas a fim de comprovar sua aplicabilidade ao SFN.

* pedro@swipetech.io
** marcelo@swipetech.io
*** eduardo@swipetech.io

Introdução

Experiências internacionais têm impulsionado a adesão mundial dos chamados pagamentos instantâneos[1] – transações que ocorrem em tempo real e permanecem disponíveis independentemente de horário comercial ou dia útil. Podem-se citar como casos mundiais já consolidados: o caso da China, em que duas empresas privadas, Tencent e Alibaba, instituíram grandes arranjos fechados[2] de escala nacional, de modo que praticamente qualquer serviço pode ser pago instantaneamente pelo celular[3] por meio dos respectivos aplicativos WeChat e Alipay; e o caso da Índia, que conta com um sistema de pagamentos instantâneos entre bancos, a *Unified Payments Interface* (UPI), mantido pelo *Reserve Bank of India*. Essas experiências se tornaram referências mundiais para que as autoridades bancárias de outros países e regiões, como Estados Unidos,[4] União Europeia,[5] e Austrália,[6] desenvolvessem suas próprias iniciativas para a implementação de pagamentos instantâneos.

Tendo em vista essas tendências, e considerando seus potenciais benefícios para a realidade brasileira,[7] o BCB tem dado os passos iniciais para definir, em teor regulatório e tecnológico, os requisitos fundamentais para um ecossistema de pagamentos instantâneos no Brasil e, posteriormente, as ações necessárias para que o SFN seja capaz de cumpri-los. Para isso, foi constituído, em maio de 2018, um Grupo de Trabalho de Pagamentos Instantâneos (GT-PI), em que são colhidas sugestões de diversos *players* do mercado, a fim de elaborar um modelo eficiente, competitivo, seguro e inclusivo.

Os requisitos fundamentais têm sido publicados em versões consecutivas no *site* do BCB.[8] O documento – atualmente na versão intermediária no momento da escrita deste relatório – define o modo de funcionamento do ecossistema e os papéis de todos os participantes da cadeia, e é a principal referência para elaboração deste trabalho.

Paralelamente, foi criado o Laboratório de Inovações Financeiras e Tecnológicas (LIFT), cujo objetivo é fomentar projetos de pesquisa e inovação tecnológica alinhados com a Agenda BC+, agenda de trabalho do BCB que inclui a implementação de pagamentos instantâneos no pilar "SFN mais eficiente". Este projeto foi um dos selecionados para a primeira edição do Laboratório. Os proponentes deste trabalho fazem parte da *fintech Swipe*[9], especializada em soluções financeiras baseadas em DLT, e têm acompanhado tanto o desenvolvimento do GT-PI[10] quanto a evolução da tecnologia DLT, que tem sido estudada por bancos centrais internacionais como uma ferramenta para a criação de sistemas de pagamentos instantâneos.

Enxergamos nesses estudos uma tendência de explorar e comparar diversas plataformas DLT, visto que ainda não se conhecem a fundo, de maneira prática, as questões envolvidas em seu uso nesses contextos.

1 Também referidos pelas expressões *fast payments*, *faster payments* e *push payments*.
2 Toda a prestação dos serviços de pagamento é realizada exclusivamente pelos próprios instituidores do arranjo. Para mais sobre arranjos, ver: https://www.bcb.gov.br/pre/bc_atende/port/arranjo.asp#3.
3 Para alguns exemplos práticos, ver: https://www.youtube.com/watch?v=O753NUrDohg.
4 https://fasterpaymentstaskforce.org
5 https://www.ecb.europa.eu/paym/target/tips/html/index.en.html
6 https://www.nppa.com.au
7 Para um resumo da iniciativa pelo BCB, ver: https://www.bcb.gov.br/htms/novaPaginaSPB/VisaoGeralPagInst.asp?IDPAI=PAGINSTA.
8 Disponível em: https://www.bcb.gov.br/htms/novaPaginaSPB/GTPagInst.asp?IDPAI=PAGINSTA.
9 https://www.swipetech.io
10 Os autores deste trabalho estiveram diretamente envolvidos nas discussões do GT-PI.

Figura 1 – Resumo dos principais estudos e Provas de Conceito (POCs) realizados por bancos centrais[11]

Entidade	Projeto	Objetivo	DLTs Utilizadas
Banco Central do Brasil	Fase 1	Identificar casos de uso e construir um protótipo de um sistema de contingência para o Sistema de Transferência de Reservas (STR) nacional.	Ethereum
	Fase 2	Analisar e comparar outras plataformas DLT para o protótipo.	Corda, Hyperledger Fabric, Quorum
Bank of Canada	Project Jasper Fase 1	Criar uma POC de um sistema de Liquidação Bruta em Tempo Real (LBTR) interbancário.	Ethereum
	Project Jasper Fase 2	Expandir as capacidades de escalabilidade e flexibilidade da POC original.	Corda
Bank of Japan, European Central Bank	Project Stella Fase 1	Investigar a capacidade de uma plataforma DLT agilizar e reduzir custos na liquidação e processamento de pagamentos.	Hyperledger Fabric
	Project Stella Fase 2	Explorar aplicações do conceito de *Delivery versus Payment* (DvP).	Corda, Elements, Hyperledger Fabric
Monetary Authority of Singapore	Project Ubin Fase 1	Desenvolver uma POC de um sistema de LBTR com uma versão digital da moeda nacional SGD.	Ethereum
	Project Ubin Fase 2	Expandir as funcionalidades da primeira POC, comparando outras plataformas.	Corda, Hyperledger Fabric, Quorum
	Project Ubin Fase 3	Explorar aplicações do conceito de *Delivery versus Payment* (DvP).	Corda, Hyperledger Fabric, Quorum, Chain
South African Reserve Bank	Project Khokha	Desenvolver uma POC de um sistema de LBTR com foco em resolver questões de privacidade e escalabilidade.	Quorum

Neste trabalho, tencionamos seguir por uma linha semelhante, introduzindo dois pontos inovadores: o uso do protocolo Stellar, uma DLT ainda pouco explorada para esse caso de uso; e uma arquitetura que faz uso de uma camada exterior focada em resolver questões de acessibilidade, segurança e privacidade da rede.

Objetivos

Este trabalho visa contribuir para o refinamento e a contínua elaboração do modelo do ecossistema de pagamentos instantâneos do Brasil. Dessa maneira, os objetivos deste trabalho são:

a) construir um protótipo que desempenhe as funcionalidades de **infraestrutura de liquidação** e ***switch***, de acordo com as definições dos requisitos fundamentais elaborados pelo BCB:

a.1) prover evidências de que a arquitetura do protótipo soluciona

11 Para uma recapitulação mais detalhada, ver: OMFIF; IBM; 2018. pp. 24-35. Resumo baseado em: SOUTH AFRICAN RESERVE BANK; 2018. p. 15.

questões relacionadas a **segurança** e **privacidade**;

a.2) prover evidências de que a arquitetura do protótipo favorece modelos de negócio **inclusivos** e **competitivos** para o ecossistema de pagamentos instantâneos brasileiro;

b) realizar testes experimentais e coletar dados para investigar a adequação do protótipo a demandas de **rapidez** e **escalabilidade**;

c) apresentar uma demonstração do protótipo, utilizando uma carteira digital para simular a interação do usuário final do ecossistema de pagamentos instantâneos.

Fundamentação Teórica

Nesta seção, são definidos os conceitos centrais para a compreensão deste projeto.

Conceitos e definições

O que é uma rede DLT? Segundo estudo do Banco Mundial:

> DLT se refere a uma abordagem inovadora e de rápida evolução para gravação e compartilhamento de dados através de múltiplas unidades de armazenamento de dados (*ledgers*), em que cada unidade possui os mesmos registros de dados e são mantidos e controlados coletivamente por uma rede distribuída de servidores, chamados nós (*nodes*). Uma maneira de pensar sobre DLT é considerá-la simplesmente uma base de dados distribuída com certas propriedades específicas. [...] Toda alteração no *ledger* é replicada em toda a rede e cada membro da rede possui uma cópia completa e idêntica de todo o *ledger* a todo momento. Este método

pode ser utilizado para gravar transações referentes a qualquer ativo representável digitalmente. [NATARAJAN; KRAUSE; GRADSTEIN; 2017. p. 1 (tradução própria)]

> "Experiências internacionais têm impulsionado a adesão mundial dos chamados pagamentos instantâneos – transações que ocorrem em tempo real e permanecem disponíveis independente de horário comercial ou dia útil."

Enxergam-se várias vantagens em potencial no uso de redes DLT,[12] como: prevenção contra gasto duplo (*double spending*); eliminação da inconsistência de saldos; aumento de rapidez e eficiência em processos; maior transparência e rastreabilidade; redução de custos com conciliação entre sistemas; e aumento de segurança. No entanto, como qualquer aplicação tecnológica, essas vantagens dependem do contexto, da implementação e dos modelos de governança associados.

Há uma variedade de redes disponíveis para serem usadas, com características distintas e projetadas para diferentes finalidades.[13] Um exemplo bem conhecido é o modelo de **redes públicas**, nas quais todos os dados permanecem disponíveis publicamente e a habilidade de contribuir para o funcionamento da rede também é aberta ao público. Essa contribuição se dá pela operação de **nós**, servidores que mantêm e atualizam cópias do *ledger*, processando adições de informação (como uma transação). Entende-se que o poder de processamento agregado dos nós ajuda a elevar a escalabilidade da rede, e que uma quantidade maior de nós contribui para que a rede seja mais resiliente: tanto se mantendo disponível caso uma parte dos nós fique fora de serviço, como preservando a integridade dos dados pelo armazenamento de cópias fidedignas do *ledger*.

Em geral, redes públicas têm como propósito criar um ecossistema descentralizado – em que não há uma única entidade responsável por manter a rede, dividindo essa responsabilidade igualmente entre todos os operadores de nós –, *peer-to-peer* e de livre acesso a usuários, bastando a um usuário da rede utilizar um serviço (como uma carteira digital), operar seu próprio nó ou conectar-se a outro nó operado por um provedor de sua escolha. Esse tipo de aplicação é o uso clássico atrelado ao termo *blockchain* e tem como seus maiores exemplos as redes que sustentam as criptomoedas Bitcoin e Ethereum.

Outro modelo de aplicação de uma rede DLT são as chamadas **redes permissionadas**, que buscam conferir as vantagens dessa tecnologia a modelos distribuídos, em que, apesar de os dados permanecerem localizados em uma base de dados compartilhada, o acesso à rede – tanto para interação quanto leitura dos dados – é controlado por uma ou mais entidades centrais por meio de credenciais de acesso, criptografia e outros métodos.

A princípio, a entidade central controla todos os nós, cedendo o direito de operá-los ou adicionar novos nós apenas a entidades autorizadas.[14] Consequentemente, usuários só podem interagir com a rede por

12 NATARAJAN; KRAUSE; GRADSTEIN; 2017. pp. 15 e 16.
13 Para uma taxonomia mais detalhada, ver: NATARAJAN; KRAUSE; GRADSTEIN; 2017. p. 13
14 OMFIF; IBM. 2018. p. 20

meio da própria entidade central ou das entidades homologadas a operar os nós, como elaborado em estudo realizado pelo Fórum Oficial de Instituições Financeiras e Monetárias (OMFIF) e IBM:

> Se um único nó [...] ficar *offline*, o sistema continua funcionando. Um sistema descentralizado não precisa que o operador central esteja *online*. Se os participantes estiverem *online*, podem continuar a enviar *tokens* de maneira *peer-to-peer* e compensar dinheiro de banco central em tempo real. [...] sistemas *blockchain* precisam ser aprimorados para superar questões de escalabilidade e velocidade. [OMFIF; IBM. 2018. p. 6 (tradução própria)]

O modelo permissionado também traz a vantagem de preservar a privacidade dos dados, garantindo que só possam ser acessados pelas partes envolvidas em uma transação e pela entidade central, por meio de uma camada externa separada da rede DLT. Esse método tem sido explorado por outros estudos de maneira bem-sucedida,[15] e neste projeto é adotada uma estrutura semelhante, como se verá a seguir no detalhamento do protótipo.

Visão geral

Esta seção aborda o modelo do ecossistema de pagamentos instantâneos, segundo as definições elaboradas pelo GT-PI e uma avaliação das tecnologias escolhidas para o protótipo.

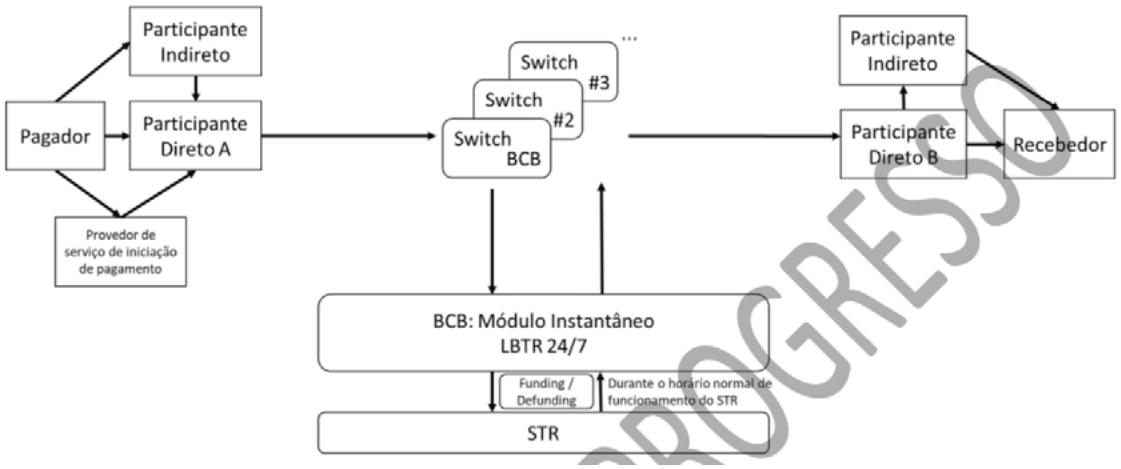
Modelo do ecossistema de pagamentos instantâneos

O protótipo toma como base o modelo elaborado pelo BCB na versão intermediária dos *Requisitos fundamentais para o ecossistema de pagamentos instantâneos brasileiro*.[16] O modelo representa um fluxo de pagamento em que ocorre, em tempo real, não apenas a autorização da transação – liberando a instrução de pagamento para um Provedor de Serviço de Pagamento (PSP) e retornando essa confirmação ao pagador – mas também a liquidação da quantia transferida, ou seja, já disponibilizando o valor para o recebedor final.

15 SOUTH AFRICAN RESERVE BANK; 2018. p. 45.

16 Disponível em: https://www.bcb.gov.br/htms/novaPaginaSPB/Requisitos%20fundamentais%20-%20vers%C3%A30%20intermedi%C3%Aria.pdf.

Figura 2 – Modelo geral do ecossistema de pagamentos instantâneos



Para esse efeito, foram definidos os seguintes papéis e suas relações, esquematizadas na Figura 2.

Lado Pagador

- **Pagador:** usuário com conta em um PSP, que inicia o pagamento.
- **Participante Direto A:** PSP do pagador, responsável por encaminhar a instrução de pagamento a um *switch*. Incluem-se como exemplos de PSPs bancos tradicionais, bancos digitais, cooperativas, instituições de pagamento, *fintechs*, entre outros.
- **Participante Indireto:** PSP que recebe a instrução de pagamento do pagador e repassa a um Participante Direto.
- **Provedor de serviço de iniciação de pagamento:** PSP contratado por um pagador para iniciar pagamentos em seu nome a partir de conta em outro PSP.

Lado Recebedor

- **Recebedor:** usuário com conta em um PSP, que recebe o pagamento.
- **Participante Direto B:** PSP do recebedor, responsável por transmitir ao recebedor a instrução de pagamento enviada pelo *switch*. Os participantes diretos A e B podem ser o mesmo PSP, ou distintos.
- **Participante Indireto:** PSP que repassa a instrução de pagamento, vinda de outro PSP, ao recebedor.

Intermediador

- ***Switch*:** serviço responsável pela transmissão da instrução de pagamento entre o PSP do pagador para a infraestrutura de liquidação, e desta para o PSP do recebedor. O BCB deve ser, pelo menos, um dos provedores desse serviço, mas também é possível que outros agentes ofertem esse serviço, desde que de maneira interoperável, ou seja, de forma que um determinado participante necessite estar conectado com apenas um agente para que seja capaz de efetivar uma transação com outro participante conectado a outro agente.

Infraestrutura de Liquidação

- **Módulo Instantâneo de Liquidação:** serviço nos quais os Participantes Diretos mantêm contas que servem de *funding* aos pagamentos instantâneos. Esse serviço é responsável por efetuar a troca dos recursos nessas contas e repassar para o *switch* o resultado (efetuado ou rejeitado) da transação. Esse serviço deve ser operado pelo BCB.
- **STR:** Sistema de Transferência de Reservas,[17] a partir do qual ocorre, em momento anterior a uma transação, a inserção de fundos nas contas dos Participantes no módulo instantâneo de liquidação.

Casos de uso

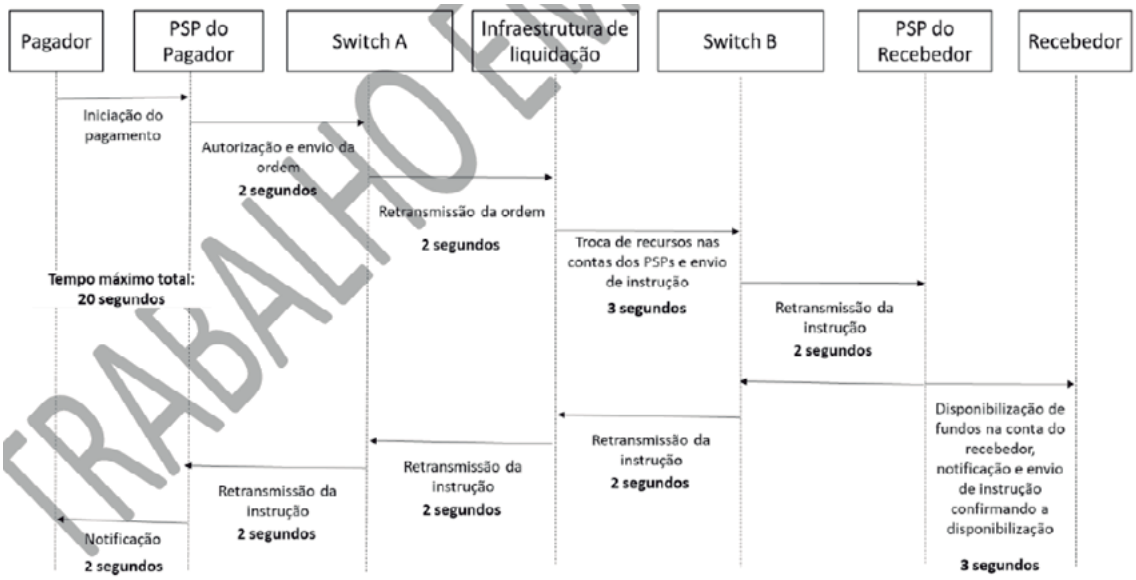
A seguir, definem-se os casos de uso a partir das condições elaboradas pelo BCB.

Pagamento instantâneo bem-sucedido

Na Figura 3, detalha-se o tempo mínimo exigido para cada etapa do processo.

17 https://www.bcb.gov.br/htms/novapaginaspb/str.asp.

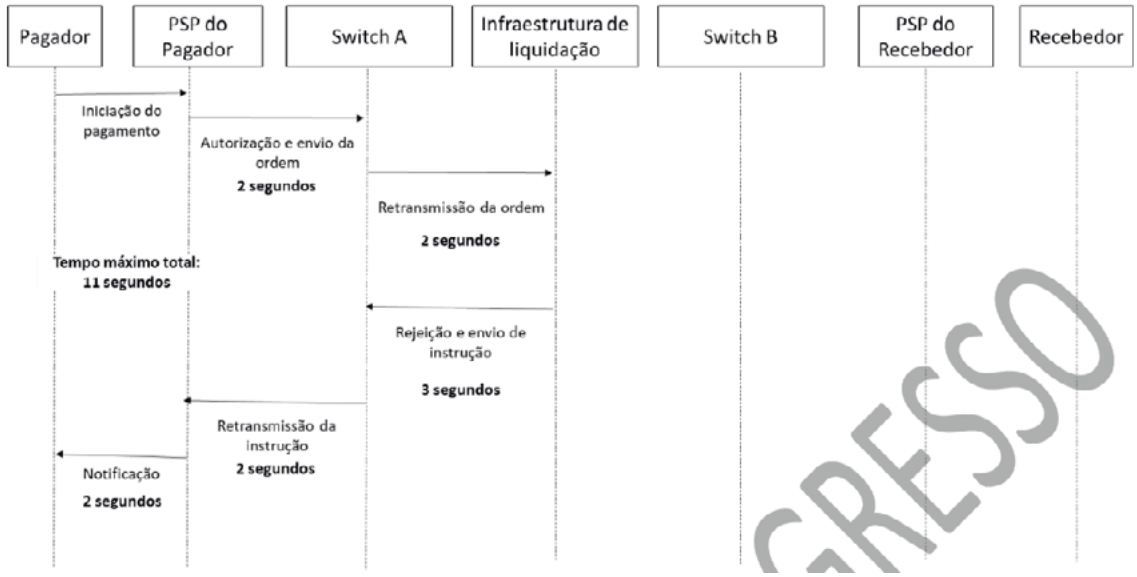
Figura 3 – Fluxo detalhando os tempos máximos de cada etapa de uma transação bem-sucedida



Dessa maneira, o caso de uso de um pagamento instantâneo bem-sucedido, do ponto de vista dos usuários, é o seguinte:

- um usuário, por meio de uma plataforma, como uma carteira digital ou similar, insere o valor que deseja enviar a outro usuário. Após o envio do pagamento, o usuário recebe em tempo real a confirmação do envio, e já consegue verificar que o valor enviado foi debitado de sua conta junto à plataforma do PSP;
- do outro lado, o usuário recebedor é notificado de que recebeu o valor transferido e já consegue movimentar o valor em sua conta na sua própria carteira digital ou similar. Essa plataforma pode ser providenciada

Figura 4 – Fluxo detalhando os tempos máximos de cada etapa de uma transação rejeitada por saldo insuficiente da conta do PSP no Módulo de Liquidação



pelo mesmo PSP do pagador, ou por um PSP distinto.

Esse fluxo ocorre, do começo ao fim, em um total de vinte segundos, no máximo, mesmo fora de horário comercial ou dia útil.

Pagamento instantâneo rejeitado por saldo insuficiente na conta do PSP

Na Figura 4, é detalhado o tempo máximo total para cada etapa do processo em caso de rejeição da transação devido à conta do PSP no Módulo de Liquidação não possuir fundos suficientes.

Assim, descreve-se esse caso de uso da seguinte maneira:

- após a ordem de pagamento ser disparada pelo usuário na plataforma do PSP, caso o PSP não detenha em sua conta no Módulo de Liquidação fundos suficientes para cumprir o pagamento, o pagamento será rejeitado pelo Módulo, repassando essa informação ao PSP de origem, que repassará ao pagador;
- esse fluxo ocorre do começo ao fim em um total de onze segundos, no máximo, mesmo fora de horário comercial ou dia útil.

Escopo do protótipo

Segue, nesta seção, uma descrição detalhada da composição do protótipo e suas funcionalidades. Durante a elaboração do protótipo, foi avaliada a ideia de utilizar uma rede DLT para fazer o papel de Módulo Instantâneo de Liquidação, e de desenvolver uma camada exterior para realizar a função de *switch*.

Tecnologias selecionadas

Rede DLT

Para a escolha de qual rede DLT utilizaríamos de fato, procuramos não nos restringir a redes tradicionalmente aplicadas em um modelo permissionado. É comum que a base de código das redes DLT seja completamente *open source*, disponível publicamente para desenvolvimento coletivo ou mesmo para ser copiado e utilizado paralelamente em projetos públicos ou privados – processo conhecido por *fork* do código. Sendo assim, algumas redes foram avaliadas segundo uma ótica focada nas **funcionalidades**, independentemente dos casos de uso a que costumam ser associadas.

Logo, considerou-se a possibilidade de reapropriar o código de uma rede pública, realizar um *fork*, e criar uma rede permissionada própria. Dessa maneira, isso traria alguns benefícios, como: utilizar uma tecnologia com vantagens já comprovadas, apoiando nas contribuições e estudo da comunidade responsável pela melhoria da rede; evitar arcar com custos por transação e criação de contas (modelo comum em redes públicas); e manter total liberdade para alterar parâmetros da rede conforme a necessidade desse caso de uso.

As plataformas avaliadas foram os DLTs Corda (https://www.corda.net), Hyperledger Fabric (https://www.hyperledger.org/projects/fabric), Ripple (XRP Ledger) (https://ripple.com), e Stellar (https://www.stellar.org). Analisando as plataformas Corda e Hyperledger Fabric, foi concluído que as capacidades do protótipo seriam limitadas pelo fato de, no funcionamento da rede, não ser criado efetivamente um ativo digital (*token*) na

rede, apenas registrando os dados das transações em base de dados locais.[18,19] Também foi cogitado realizar um *fork* permissionado a partir da rede Ripple ou da rede Stellar.

Chegou-se à conclusão de que, para os fins deste projeto, apesar de ambas as redes serem semelhantes em quesito de funcionalidades, a rede Stellar é intrinsicamente voltada para a criação e customização de *tokens*,[20] ao contrário da rede Ripple, que foca no uso da criptomoeda XRP para remessas internacionais. Portanto, a rede Stellar pareceu mais recomendada para se ter total controle sobre as funcionalidades da moeda transacionada.

Assim, foi decidido criar uma rede permissionada a partir do código da rede **Stellar**, que possui as seguintes vantagens:

- rapidez: as transações demoram ao todo uma média de 3 a 5 segundos, desde a autorização até a compensação;[21]
- escalabilidade: o processamento da rede atinge consistentemente 1.000 transações por segundo, sendo capaz de 4.000 t/s sem alterações no código.[22] Além disso, testes realizados pela Deloitte relataram atingir um processamento de 10.000 t/s.[23]

Deve-se levar em consideração que esses dados são apenas aplicáveis à rede pública, que conta com aproximadamente 400 nós ativos atualmente.[24] No caso de uma rede permissionada, não é claro como a performance da rede pública se traduziria para um *fork* permissionado, já que depende do poder de processamento dos nós e do *hardware* utilizado. Para esclarecer essa questão, foram incluídos testes de escalabilidade em nossas hipóteses, como se pode ver na seção "Resultados" deste relatório.

Ao longo deste estudo, referimos a nossa rede permissionada baseada em código Stellar como **Rede *Swipe***.

Camada exterior

Foi desenvolvido um componente, chamado de **Camada *Swipe***, para desempenhar as seguintes funcionalidades:

- função de *switch*: realizar a comunicação entre a rede e participantes externos;
- acessibilidade: por meio de uma API e SDKs, abstrair os conceitos específicos da rede, facilitando sua integração e uso;
- segurança: implementar um controle de acesso a dados por meio de credenciais;
- privacidade: implementar criptografia de ponta a ponta para todos os dados, de forma que as informações fiquem disponíveis apenas aos usuários envolvidos nas transações e à entidade central que opera a rede.

As técnicas específicas utilizadas para prover essas funcionalidades são descritas na subseção "Descrição Técnica".

18 HEARN; 2016. pp. 25-26
19 ANDROULAKI; BARGER; BORTNIKOV et al. 2018. pp. 10-12
20 https://www.stellar.org/blog/tokens-on-stellar/
21 https://www.stellar.org/how-it-works/stellar-basics/
22 https://stellar.stackexchange.com/questions/334/scalability-on-stellar-network
23 https://www.americanbanker.com/news/how-barclays-aims-to-bring-a-billion-unbanked-into-the-fold
24 Dados recolhidos diretamente da rede em 9 nov. 2018.

Modelo do protótipo

O escopo do protótipo se baseia nas funções de Módulo Instantâneo de Liquidação e *switch*. Na Figura 5, apresenta-se um modelo adaptado do esquema apresentado pelo BCB. A partir dele, foi elaborado o modelo do protótipo (Figura 6), substituindo os papéis do ecossistema pelos componentes respectivos.

Figura 5 – Modelo do ecossistema de pagamentos instantâneos

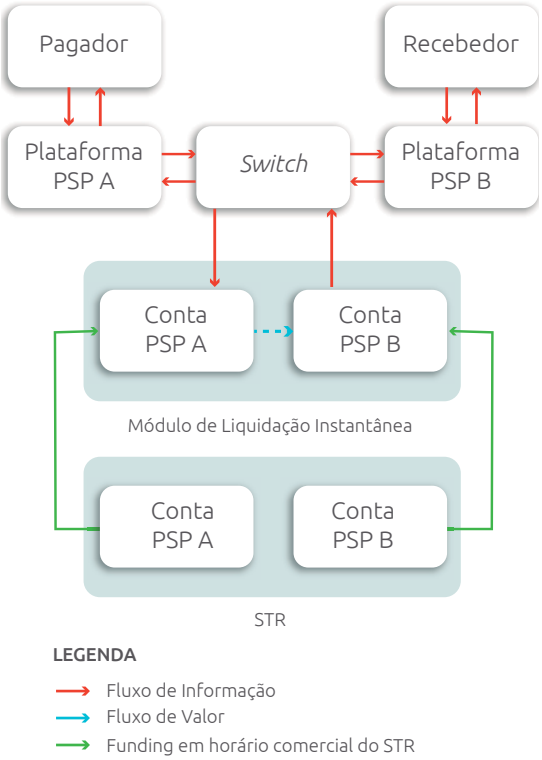
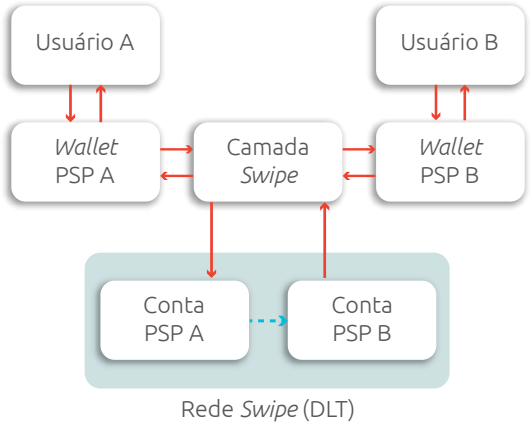


Figura 6 – Modelo do protótipo



Para a representação da plataforma de cada PSP, foi desenvolvido um protótipo de carteira digital, chamado *Wallet*, pelo qual um usuário pode enviar ou receber pagamentos instantâneos, bem como visualizar seu saldo e histórico de transações em tempo real.

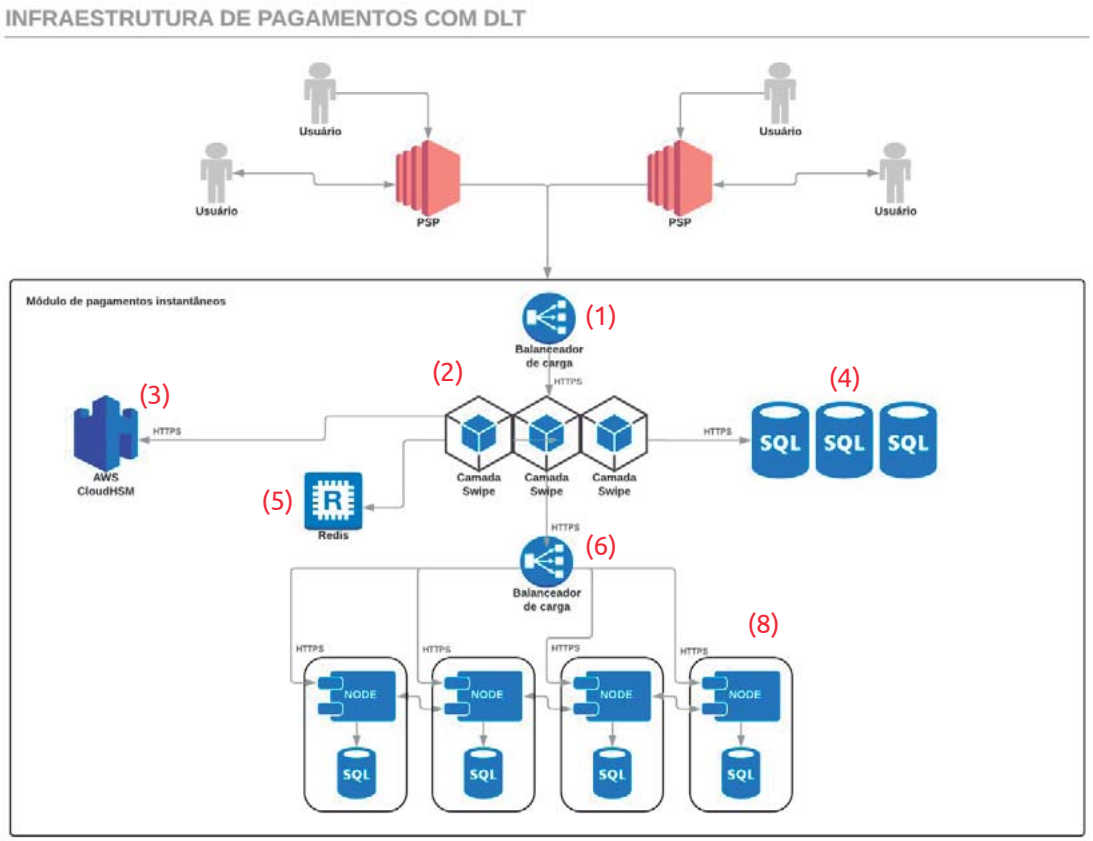
Deve-se notar que, para esse protótipo, considera-se um momento posterior ao *funding* realizado a partir do STR, não cabendo ao escopo desse protótipo uma simulação dessa parte do fluxo.

Descrição técnica

A Figura 7 detalha a arquitetura tecnológica do protótipo, acompanhada das definições de seus componentes a seguir:

1. **Balanceador de carga:** distribui as requisições enviadas pelo PSP entre instâncias redundantes da Camada *Swipe*.
2. **Camada *Swipe*:** abstrai o acesso à rede, serve como ponto de conexão de todo o sistema e garante a segurança e privacidade dos dados.
3. ***Hardware Security Module*:** armazena chaves criptográficas e informações confidenciais da aplicação.
4. **Banco de Dados Relacional:** armazena dados necessários para o funcionamento da Rede *Swipe*.
5. **Camada de *Cache*:** armazena dados temporários para otimização da performance.
6. **Balanceador de carga:** distribui as requisições para os nós da rede DLT;
7. **Nós da Rede *Swipe*:** são responsáveis pelo processamento da rede, garantindo a consistência das transações, saldos das contas e atualização em tempo real do *ledger*.
8. ***Bucket*:** armazena cópias periódicas do *ledger*, fortalecendo a redundância do sistema e facilitando a entrada de nós na rede.

Figura 7 – Arquitetura do protótipo



Considerações de segurança e privacidade

É fundamental que a plataforma esteja protegida contra fraudes e participantes maliciosos. Para isso, foram tomadas medidas para identificar e prevenir potenciais brechas no fluxo de informação que poderiam comprometer o sistema.

Toda comunicação interna e externa é feita **exclusivamente via protocolo HTTPS com HSTS**[25] **habilitado**, de forma que todos os dados sejam sempre trafegados em conexões encriptadas, garantindo proteção a ataques como *Man-in-the-Middle*.[26]

O acesso entre os recursos da nossa arquitetura é controlado por meio de *firewalls* e redes privadas. Isso significa que só é permitida a conexão direta entre os componentes internos da aplicação cuja comunicação direta é essencial para seu funcionamento.

Os dados armazenados no componente (4) Banco de Dados Relacional são salvos e protegidos com criptografia AES (*Advanced Encryption Standard*).[27] Assim, eventuais acessos indevidos a essa camada não garantem o recolhimento de informações úteis sobre as transações ou participantes da rede.

Cada participante interage com o sistema por meio de um ou mais pares de credenciais. A Figura 8 detalha quais ações cada participante do sistema consegue realizar por meio de suas credenciais e, consequentemente, as informações a que tem acesso.

25 https://https.cio.gov/hsts
26 https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
27 https://www.cyclonis.com/what-is-aes-256-encryption/

Figura 8 – Perfis de acesso

Participantes / Ações Possíveis	BCB – Entidade Controladora da Rede	Órgãos Competentes (Receita Federal, COAF)	PSP	Swipe – Desenvolvedora da Rede
Criar novas credenciais de acesso	Sim	Não	Não	Não
Visualizar saldos de todas as contas	Sim	Sim, condicionado pelo BCB	Não	Não
Visualizar o histórico de transações de toda a rede	Sim	Sim, condicionado pelo BCB	Não	Não
Visualizar saldo de sua própria conta	N/A	N/A	Sim	N/A
Visualizar o próprio histórico de transações	N/A	N/A	Sim	Não
Iniciar um pagamento a partir de sua própria conta	N/A	N/A	Sim	N/A
Iniciar um pagamento a partir de outras contas	Não	Não	Não	Não

Assim, tencionou-se criar um modelo que garanta segurança e privacidade dos dados, desde que cada participante siga boas práticas de segurança de *software* para proteção de suas credenciais.

Resultados

Para investigar a adequação do protótipo a demandas de rapidez e escalabilidade, entendidas como essenciais para o funcionamento de pagamentos instantâneos, foram definidas hipóteses e realizados testes com diferentes cenários e configurações para sua validação.

Hipóteses

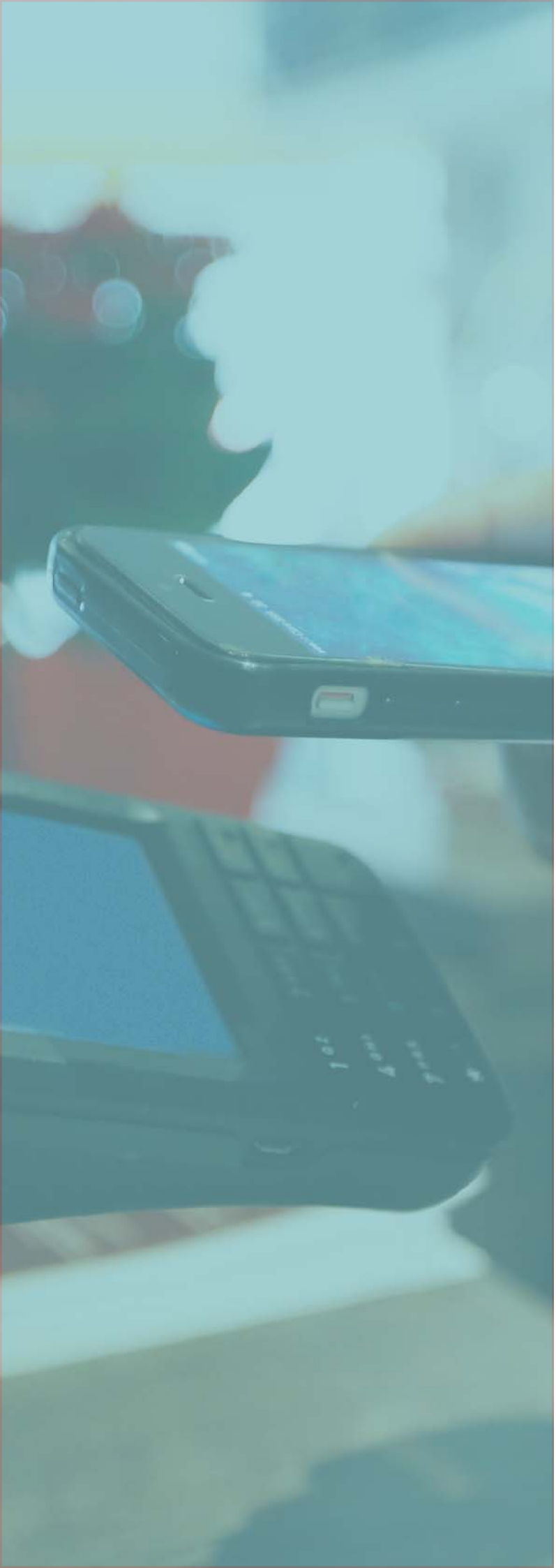
As hipóteses definidas para o protótipo foram as seguintes:

1. o tempo médio total decorrido para um fluxo de um pagamento bem-sucedido deve ser igual ou menor a **dezoito** segundos;
2. o tempo médio total decorrido para um fluxo de um pagamento rejeitado por saldo insuficiente na conta do PSP deve ser igual ou menor a **nove** segundos;
3. o protótipo deve suportar **105 transações por segundo** sem ultrapassar a faixa de dezoito segundos para o processamento médio de cada transação.

Explica-se a seguir como as hipóteses foram fundamentadas.

Para realizar uma simulação mais próxima possível de uma situação real, foi desenvolvido um *script* – uma lista predeterminada de comandos a serem executados – para simular a iniciação de pagamentos por parte de múltiplos pagadores simultâneos a múltiplos recebedores. Dessa maneira, o tempo considerado para as hipóteses referentes a rapidez (hipóteses 1 e 2) deve tomar como base todo o fluxo dos casos de uso apontados anteriormente, **exceto** a notificação do pagador por parte do PSP do pagador, cujo tempo mínimo é de dois segundos, como definido anteriormente nas figuras 3 e 4. Como essa etapa do processo compete somente à relação entre o pagador e seu PSP, não cabe ao escopo deste protótipo.

Para a hipótese referente à escalabilidade (hipótese 3), foi tomado como referência o número recorde de transações processadas



pelo Sistema de Transferência de Fundos (Sitraf), entidade responsável pelo processamento da TED, em um dia: 5.034.419 mensagens de pagamento.[28] Para fazer uma estimativa de qual seria o processamento médio necessário para cobrir essa demanda, dividiu-se esse número pelo tempo de operação diário do Sitraf – 13 horas e 25 minutos,[29] ou 48.300 segundos:

$$5.034.419 \div 48.300 \cong 105 \text{ transações/segundo}$$

Testes e validação das hipóteses

Hipótese 1

Para o teste da Hipótese 1, foram preparados cinquenta *batches* compostos de cem transferências cada. Cada *batch* foi disparado um segundo após o *batch* anterior ter sido processado por completo. Foram medidos os tempos individuais de processamento da Camada *Swipe*, Rede *Swipe* e a latência para cada transação, resultando num *corpus* de dados de 5.000 transações realizadas com sucesso.

A Figura 9 mostra o tempo de processamento médio para cada etapa do processo, considerando todas as 5.000 transações.

Figura 9 – Tempo de processamento para transações bem-sucedidas

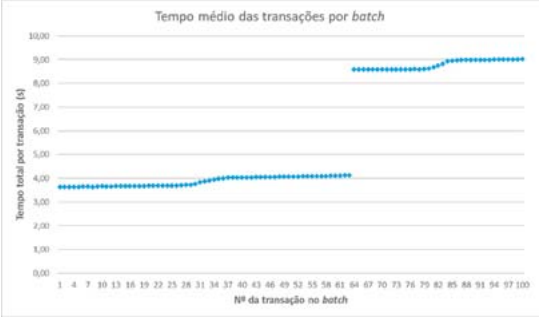
Tempo de Processamento (Médias Totais)				
Unidade	Camada Swipe	Rede Swipe	Latência	Total
ms	86	4039	1564	5689
%	1,5%	71,0%	27,5%	100,0%

28 https://www.cip-bancos.org.br/Paginas/SITRAF-bate-novo-recorde.aspx

29 https://www.cip-bancos.org.br/ProdutosIMF/Regulamento%20Operacional%20-%20SITRAF.pdf

Pode-se observar que o tempo médio total para processamento de cada transação foi de aproximadamente **5,7 segundos**, estando abaixo da meta de dezoito segundos, o que confirma a hipótese como válida.

Convém observar que o tempo de processamento interno a cada *batch* não foi uniforme, tendendo a um aumento para as últimas transações de cada *batch*. O gráfico a seguir mostra o tempo médio de cada transação por *batch*.



Como se observa no gráfico, além de um aumento gradual no tempo levado por transação, houve um aumento brusco a partir da transação 64 de cada *batch*.

O aumento gradual pode ser explicado pelo aumento na carga de processamento ao longo dos *batches*. Por exemplo, ao receber a 1ª transação do *batch*, as máquinas possuem maior poder de processamento disponível para realizar a operação. Porém, ao receber a 50ª transação do *batch*, há menos poder de processamento disponível devido ao processamento das transações anteriores. O aumento repentino pode estar associado ao tempo de fechamento de cada *ledger* processado pela rede, que ocorre a cada cinco segundos. Essa tendência de aumento pode ser um ponto a ser abordado em futuras otimizações do protótipo.

Hipótese 2

Para o teste da Hipótese 2, foram preparados *batches* idênticos aos utilizados na Hipótese 1, com a diferença de que as contas não possuíam saldo suficiente para cumprir as transações. Foram feitas as mesmas medições aplicadas à hipótese anterior.

A Figura 10 mostra o tempo de processamento médio para cada etapa do processo:

Figura 10 – Tempo de processamento para transações rejeitadas por saldo insuficiente

Tempo de Processamento (Médias Totais)				
Unidade	**Camada Swipe**	**Rede Swipe**	**Latência**	**Total**
ms	102	4128	1564	5794
%	1,8%	71,2%	27,0%	100,0%

Como se pode observar, o tempo médio total para processamento de cada transação foi de aproximadamente **5,8 segundos**, estando abaixo da meta de nove segundos, confirmando a hipótese como válida.

Devido ao mesmo fenômeno observado no teste da Hipótese 1, o tempo máximo decorrido para uma transação foi de 10,29 segundos, e o tempo mínimo foi de 3,15 segundos. Foi observado que 6% das 5.000 transações excederam o tempo de nove segundos. Entende-se isso como uma ressalva à validade da hipótese e como um ponto para aprimoramento do protótipo.

É interessante notar que os tempos médios de processamento foram praticamente idênticos aos medidos no teste da Hipótese 1. Isso pode ser explicado pelo modo de funcionamento da rede, em que não há diferença significativa entre as operações necessárias em caso de sucesso ou de rejeição de uma transação.

Hipótese 3

Para o teste da Hipótese 3, foram preparados trinta *batches* compostos de 105 transferências cada. Diferentemente

das hipóteses anteriores, cada *batch* foi disparado um segundo após o *batch* anterior ser **enviado**, ou seja: mantendo uma frequência constante de 105 transações por segundo. O *corpus* resultante consistiu de um total de 3.150 transações.

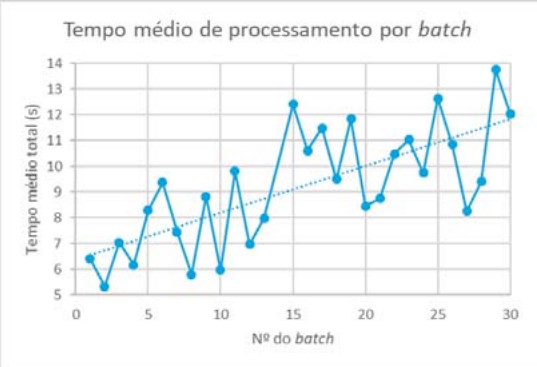
A Figura 11 mostra o tempo de processamento médio para cada etapa do processo:

Figura 11 – Tempo de processamento para transações no teste de escalabilidade

Tempo de Processamento (Médias Totais)				
Unidade	**Camada Swipe**	**Rede Swipe**	**Latência**	**Total**
ms	1687	7415	80	9182
%	18,4%	80,8%	0,9%	100,0%

Em primeiro lugar, foi observado que todas as transações foram realizadas com sucesso. Além disso, pode-se ver que o tempo médio das transações foi de aproximadamente9,2 segundos, abaixo da meta de 18 segundos. Esses fatos em conjunto confirmam a hipótese como válida.

Deve-se notar que novamente foi observado o fenômeno de aumento do tempo das transações ao longo de *batches* individuais. Nesse teste, tal fenômeno foi agravado pelo fato de cada *batch* ter sido disparado antes do término dos *batches* anteriores. Isso pode ser observado no gráfico a seguir. Essa tendência de aumento pode ser um ponto a ser abordado em futuras otimizações do protótipo.



Características inovadoras

Identificamos que a escolha pelo modelo proposto para compor a infraestrutura de liquidação e *switch* – uma rede DLT munida de uma camada exterior – proporciona benefícios particulares, como:

- **rastreabilidade**: todo o histórico das transações é registrado na própria rede e permanece à disposição da entidade central – o BCB e demais órgãos regulatórios como Conselho de Controle de Atividades Financeiras (Coaf) e Receita Federal – para verificação e controle;
- **redundância dos dados**: os dados se concentram em não apenas um servidor central, mas em vários nós distribuídos, de forma que, caso haja perda de dados por parte de um nó ou conjunto de nós, isso não compromete a integridade dos dados do restante da rede;
- **disponibilidade**: caso mais da metade dos nós da rede se tornem *offline* (o que inclui os nós específicos da entidade central), a rede permanece em funcionamento e disponível para acesso, sendo prejudicado apenas seu poder de processamento;
- **privacidade**: a adição da camada exterior provê privacidade aos usuários, ao mesmo tempo em que permite à entidade central o acesso aos dados;
- **prevenção contra inconsistências e fraudes**: como os dados são constantemente validados por todos os nós da rede, em sistemas DLT é virtualmente impossível a falsificação maliciosa de dados. Pelo mesmo motivo, o próprio funcionamento

do sistema evita a necessidade de conciliação bancária e ocorrência de gasto duplo (*double spending*),

- **interoperabilidade**: a Camada *Swipe* é munida de *Software Development Kits* (SDKs) e uma *Application Program Interface* (API), o que possibilita a integração com sistemas por meio de comunicação baseada na convenção *Representational State Transfer* (Rest), altamente utilizada. Assim, a integração com a rede exige esforços mínimos se comparada com redes que não dispõem de APIs, o que facilita a integração com sistemas legado e é positivo para que o ecossistema de pagamentos instantâneos permaneça inclusivo a outros *players* do mercado.

Contribuição para o SFN

A implementação de um ecossistema de pagamentos instantâneos traria diversos pontos positivos para o SFN. Segundo o BCB,[30]

> O Banco Central do Brasil (BCB) entende que existem algumas lacunas na cesta de instrumentos de pagamento disponíveis para a população brasileira, como, por exemplo:
>
> (i) a utilização elevada do dinheiro em espécie para pagamentos de serviços entre particulares e para transferências de recursos entre pessoas físicas, o que justifica a política do BC de incentivo à eletronização dos instrumentos de pagamento de varejo, tendo em conta que podem gerar redução significativa do gasto anual com a realização de pagamentos;
>
> (ii) as transferências eletrônicas interbancárias de crédito, como a TED e o DOC, estão longe do seu potencial de utilização, principalmente por causa das tarifas elevadas, para essas operações, das dificuldades no endereçamento das transferências e da ausência de confirmação das transações; e
>
> (iii) os custos de aceitação de cartões de crédito e de débito são muito elevados e a disponibilização dos recursos para o beneficiário final do pagamento demora muito tempo.
>
> O BCB entende que os pagamentos instantâneos têm o potencial de ser a solução inovadora que ajudará a preencher as lacunas identificadas.

Com a implementação de um ecossistema eficiente, competitivo, seguro e inclusivo, identificam-se vários ganhos para cada participante:

- **usuário pagador**: custo de transação reduzido em relação a métodos atuais, o que também viabiliza micropagamentos; disponibilidade ininterrupta do serviço; maior gama de canais de acesso; canais de acesso mais inclusivos (ambiente *open banking*), atendendo, por exemplo, a população desbancarizada; facilidade de endereçamento dos pagamentos, sendo necessário um número mínimo de informações sobre o recebedor; recebimento imediato de notificação do sucesso ou rejeição do pagamento; transparência na cobrança de eventuais tarifas sobre a transação; habilidade de pagamentos mesmo entre usuários com contas em diferentes PSPs;

30 Texto retirado de: https://www.bcb.gov.br/htms/novaPaginaSPB/VisaoGeralPagInst.asp?IDPAI=PAGINSTA.

- **usuário recebedor**: habilidade de iniciar o pagamento por parte do recebedor; otimização do fluxo de caixa devido à disponibilização imediata dos recursos, diminuindo a necessidade de obtenção de crédito; identificação do pagador; a padronização do código identificador facilita o recebimento de pagamentos; possibilita a existência de um código identificador único para o recebedor, de modo que o pagamento seja realizado da mesma forma independente do PSP utilizado pelo pagador; estimula novos serviços devido à viabilidade de micropagamentos;
- **PSPs**: possibilidade de ofertar um serviço mais vantajoso para pagadores e recebedores; possibilidade de ofertar novos serviços adicionais; aumento na competitividade em relação a instituições financeiras tradicionais; modelo de negócio facilita a criação de ambientes *open banking*;
- **agentes provedores de *switch***: possibilidade de usufruir de um mercado aberto a novos *players*, conectando de maneira interoperável ao *switch* operado pelo BCB; possibilidade de agregar serviços adicionais como prevenção antifraude, entre outros;
- ***fintechs* com demais funções**: possibilidade de oferecer serviços agregados ao serviço básico de pagamento, como oferta de seguros, crédito, investimentos, conciliação, pagamentos de tributos, serviço de iniciação de pagamentos, entre outros;
- **governo, BCB e sociedade**: redução de custos com papel-moeda; estímulo à economia; estímulo à criação de um ambiente *open banking*; prevenção contra crimes financeiros; maior transparência para órgãos reguladores; SFN com arquitetura mais robusta.

Restrições

Esta seção trata de pontos que, apesar de serem entendidos como requisitos fundamentais para o ecossistema de pagamentos instantâneos, não foram testados com o protótipo neste estudo. Portanto, são feitas considerações quanto à viabilidade de próximos testes desses requisitos. Adicionalmente, citam-se como sugestões para próximos estudos alguns recursos complementares comumente associados pela literatura às capacidades de redes DLT permissionadas.

Restrições do protótipo quanto aos requisitos fundamentais

Interoperabilidade entre *switches* adicionais

Um requisito fundamental apontado para o *switch* é:

> No âmbito do ecossistema de pagamentos instantâneos, caso existam agentes, além do BCB, ofertando serviço de *switch*, deve existir interoperabilidade ampla, multilateral e irrestrita entre eles, de forma a possibilitar que um determinado participante necessite estar conectado com apenas um agente para que ele seja capaz de efetivar uma transação com outro participante que esteja conectado com outro agente. [...] Esse modelo implica

que é possível a existência concomitante de diversos agentes que ofertem serviço de *switch*.

Apesar de não caber ao escopo deste protótipo isolado comprovar a interoperabilidade entre *switches* adicionais, a Camada *Swipe* disponibiliza API e SDKs para integração com outros agentes provedores de *switch*.

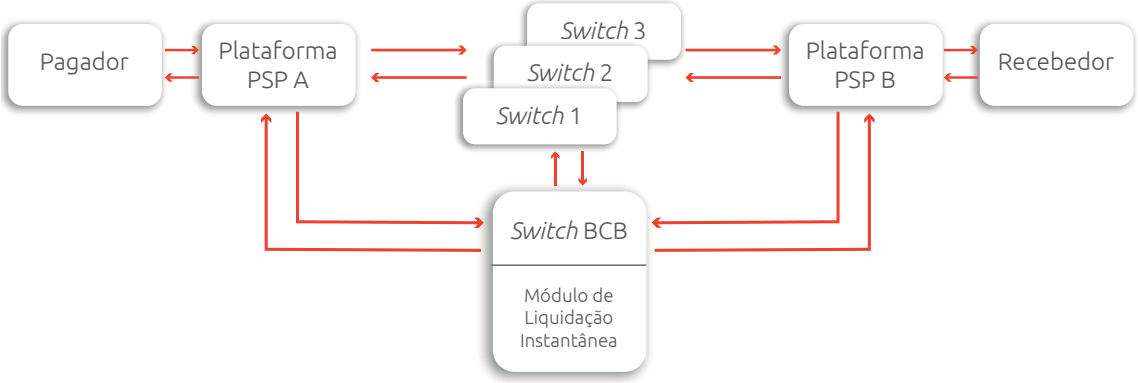
No entanto, o funcionamento do protótipo é tal que esses *switches* adicionais **não** seriam intercambiáveis ao *switch* operado pelo BCB, situando-se, em vez disso, entre o *switch* do BCB e o PSP a que está conectado (relação esquematizada na Figura 12). Assim, os PSPs podem conectar-se diretamente ao *switch* do BCB, ou podem conectar-se a um *switch* operado por terceiros (para, por exemplo, usufruir de serviços adicionais) que, por sua vez, realizam sua comunicação com o restante do ecossistema por meio do *switch* do BCB.

Há alguns motivos pelos quais essa operação é necessária:

- a Camada *Swipe* provê, além da função de *switch*, camadas adicionais de acessibilidade, privacidade e segurança que são essenciais para o bom funcionamento do sistema. Caso a interoperabilidade entre *switches* dependesse da substituição da Camada *Swipe*, o custo de desenvolvimento para demais *switches* seria mais elevado e extrapolaria suas obrigações fundamentais, prejudicando a competitividade desse serviço;
- para ser possível o endereçamento de contas a partir de informações como CPF, *e-mail* ou número de telefone, é preciso que haja uma base de dados relacional que contenha e identifique essas informações. Para garantir a privacidade dos usuários, deve ser o *switch* do BCB – entidade neutra e sem fins lucrativos –, e não de terceiros, a realizar essa operação.

Para aumentar a resiliência do sistema, de forma que haja mais de um provedor das funções realizadas pela Camada *Swipe*, enxerga-se a possibilidade de o BCB outorgar, por meio de licitação pública ou processo semelhante, o direito de operar instâncias adicionais da Camada *Swipe* a outras entidades que julgar adequadas. Dessa maneira, em caso de uma eventual indisponibilidade por parte da instância operada pelo BCB, a rede continuaria a operar com todas as suas funcionalidades intactas.

Figura 12 – Esquema da relação entre *switches* segundo o funcionamento do protótipo



Funcionamento do *funding* a partir do STR

Um requisito fundamental apontado pelo BCB para a infraestrutura de liquidação é:

> [...] existirá uma conta específica para cada participante para servir de *funding* para os pagamentos instantâneos e que poderá ser livremente movimentada no horário normal de funcionamento do STR. Quando o STR estiver fechado, o montante alocado previamente na conta deverá ser suficiente para viabilizar a efetivação dos pagamentos. O acesso a essas contas funcionaria por meio de um novo sistema independente do STR. A transferência de recursos entre os PSPs mobilizaria exclusivamente o saldo dessas contas.

Nosso protótipo considerou um momento posterior ao *funding* das contas, já que seria necessário realizar experimentos com um ambiente de testes real do STR para comprovar a possibilidade desse processo. No entanto, novamente supõe-se isso ser possível, devido à disponibilidade de integração via API.

Próximos passos

Nesta seção, trata-se de tendências futuras exploradas por outros estudos quanto ao uso de redes DLT para infraestrutura de sistemas de pagamento nacionais. Apontam-se recursos e funcionalidades que o protótipo desenvolvido para esse projeto pode vir a desempenhar após mais desenvolvimento e aprimoramento. Deve-se considerar esta seção como uma série de sugestões para próximos projetos e provas de conceito.

Futuros testes e otimizações

Neste projeto, as hipóteses e os testes foram definidos com base em uma avaliação preliminar de uma implementação de DLT para o caso de uso abordado. Próximos projetos poderiam abordar pontos revelados pelos testes, como o aumento entre *batches* do tempo de processamento das transações. Há diversas vias para o contínuo desenvolvimento do protótipo, como: otimizar o código, otimizar a conexão entre componentes da infraestrutura, experimentar diferentes configurações de processamento da infraestrutura e explorar outros cenários de teste mais aprofundados.

CBDC (Moeda Digital de Banco Central)

Ao longo da elaboração deste estudo, identificou-se uma semelhança entre o modelo do protótipo e as propriedades de uma Moeda Digital de Banco Central (CBDC, na sigla em inglês), às vezes referida pela literatura como Moeda Fiduciária Digital (DFC, na sigla em inglês).[31] Segue aqui uma explicação dos diferentes tipos de CBDCs, suas propriedades, e como isso pode ser explorado a partir do protótipo.

O modelo de nosso protótipo implica a criação de uma moeda digital (também chamada neste contexto de *token*) emitida pelo BCB que seria usada diretamente por instituições financeiras para liquidação. Isso seria parte de uma mudança de paradigma em relação ao modo como esse processo é realizado atualmente. Segundo estudo da *Official Monetary and Financial Institutions Forum* (Omfif) e da *International Business Machines* (IBM),

30 Como em Burgos e Batavia (2018).

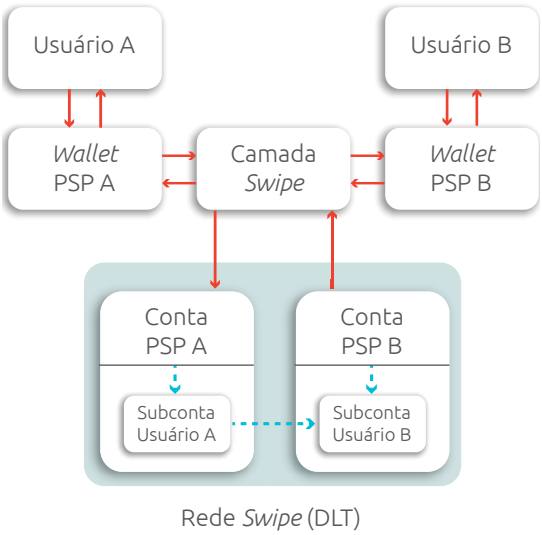
> Tradicionalmente, as formas de dinheiro emitidas por bancos centrais, bancos comerciais e emissores privados são baseadas em contas, o que significa que os saldos são registrados em um livro de contas. Neste sistema, os débitos e créditos das contas ocorrem sem a transferência de valor real. Uma **CBDC de atacado** substitui o dinheiro atualmente usado para liquidar transações interbancárias (reservas mantidas por bancos junto ao banco central) por um *token* digital. [...] Isso permitiria o empréstimo/transferência de liquidez entre instituições bancárias e não bancárias, para aliviar pressões de liquidez acumuladas no sistema, bem como reduzir o risco de contraparte associado a tempos extensos de liquidação. [OMFIF; IBM. 2018. pp. 10-11 (tradução e destaque próprios)]

Assim, identificou-se que o protótipo se baseia na criação de uma **CBDC de atacado**: uma moeda digital emitida pelo BCB que seria utilizada para liquidação entre instituições financeiras. Com isso em mente, procurou-se dar um passo adiante e discutir como seria um modelo que permitisse a circulação de uma **CBDC de varejo**, em que a moeda emitida seria utilizada diretamente pelo usuário final.

Uma CBDC de varejo agiria como uma substituição do papel-moeda, sendo usada igualmente em todos os contextos de transações entre pessoas físicas, pessoas jurídicas e entidades do governo. Segundo esse modelo, também seriam possíveis transações *peer-to-peer*, ou seja: envolvendo o mínimo de intermediários entre o pagador e o recebedor.

Para esse efeito, foi elaborado, a partir do modelo do protótipo, um modelo de subcontas, segundo esquema da Figura 13.

Figura 13 – Esquema do modelo de subcontas



Nesse modelo, são criadas na rede DLT subcontas referentes aos usuários de cada PSP. Essas subcontas são subordinadas às contas dos PSPs, que são as únicas entidades autorizadas a movimentá-las. As subcontas dos usuários não precisam de *funding* para funcionamento, tendo saldo zero, exceto durante uma transação. No momento da transação, são transferidos fundos na sequência PSP A → Subconta Usuário A → Subconta Usuário B → PSP B.

Assim, conquistam-se alguns benefícios inerentes às CBDCs de varejo, como permitir a rastreabilidade ponta a ponta de todas as transações. A Figura 14 mostra um exemplo de como uma transação seria registrada no *ledger* da rede, considerando o modelo utilizado no protótipo; e a Figura 15 demonstra também um exemplo no caso do modelo de subcontas.

Figura 14 – Registro de uma transação no *ledger* com uma CBDC de atacado

Operation	Details	Date
85774645839577089	PSP A transferred 30.00 BRL to PSP B.	13 Sep 2018 21:10:24 UTC

Figura 15 – Registro de uma transação no *ledger* com uma CBDC de varejo

Operation	Details	Date
85774645839540225	PSP A transferred 30.00 BRL to User A.	13 Sep 2018 21:10:24 UTC
85774645839572993	User A transferred 30.00 BRL to User B.	13 Sep 2018 21:10:24 UTC
85774645839577089	User B transferred 30.00 BRL to PSP B.	13 Sep 2018 21:10:24 UTC

Comparando os dois exemplos, percebe-se que o modelo de subcontas garantiria transparência ponta a ponta nas movimentações, rastreando o fluxo tanto pelo PSP como até o usuário, o que pode ser avaliado como uma ferramenta das entidades reguladoras contra crimes financeiros.

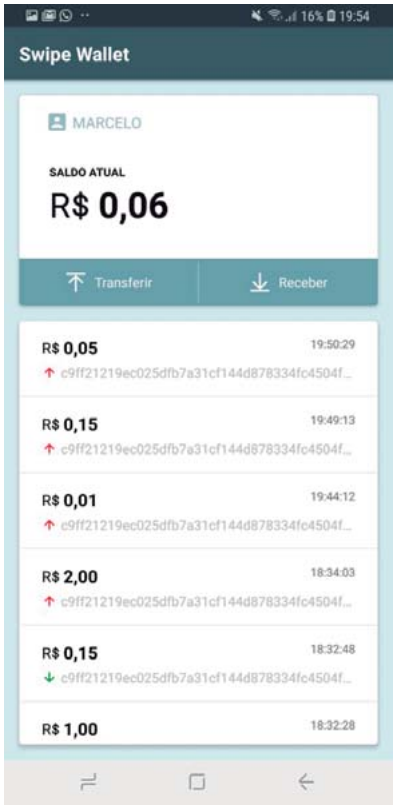
O modelo de subcontas também seria providencial para possibilitar transações *peer-to-peer*. Por exemplo, o BCB poderia instituir seu próprio serviço de pagamentos, disponibilizando gratuitamente para cidadãos brasileiros sua própria carteira digital de pagamentos instantâneos. Dessa maneira, a moeda digital poderia ser circulada livre e autonomamente entre os cidadãos sem a necessidade de intermediários adicionais.

Na demonstração do protótipo, foi desenvolvida uma carteira digital em que é possível visualizar essa experiência por parte do usuário final. Apresentam-se, na Figura 16, as etapas desse fluxo segundo a operação da carteira digital.

Figura 16 – Fluxo de pagamento instantâneo *peer-to-peer* do ponto de vista do usuário

Após o pagador identificar o recebedor por meio de leitura de um *QR Code* ou outro método de endereçamento, o pagador informa o valor a ser transferido e confirma a transação.

O pagador recebe, em tempo real, um recibo confirmando o resultado do pagamento. As informações do recibo podem ser definidas para serem identificadas com facilidade, utilizando por exemplo CPF, *e-mail*, número de celular, entre outros.



O pagador consegue ver em seu histórico de transações a transação executada e seu saldo atual.

Uma notificação da transação é enviada, em tempo real, para a carteira do recebedor, que consegue confirmar, por meio de um recibo, a identidade do pagador.

Com esse exemplo prático, espera-se demonstrar que é possível realizar um ecossistema de pagamentos instantâneos que permite tanto transações por meio de intermediários como transações *peer-to-peer*.

Modelos inovadores de liquidação

Pensando na contínua evolução do SFN, convém considerar inovações permitidas pelo uso de DLT, além do ecossistema de pagamentos instantâneos.

O uso de uma rede DLT possibilita a criação de diversas variedades de ativos digitais. As CBDCs são um exemplo de um ativo digital pareado à moeda fiduciária. No entanto, não há limitação tecnológica para também serem representados ativos como títulos – ações, debêntures, títulos de propriedade, entre outros.[31]

Com base nisso, estudos[32] têm avaliado a implementação de mecanismos de **Delivery VS Payment** (DvP): um procedimento de liquidação no qual títulos e moedas são trocados simultaneamente para garantir que a entrega dos títulos ocorra

31 OMFIF; IBM. 2018. p. 12

32 http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-and-SGX-successfully-leverage-blockchain-technology-for-settlement-of-tokenised-assets.aspx

apenas no momento em que o pagamento correspondente for realizado.

Outra implementação, vista como um passo adiante ao DvP, é o chamado ***Payment VS Payment*** (PvP): um método semelhante ao DvP em que, em vez de títulos, são trocadas duas moedas distintas. Enxergam-se como caso de uso as trocas monetárias internacionais. Essa implementação teria um desafio adicional, pois depende da interoperabilidade entre diferentes *ledgers* – como os sistemas financeiros nacionais de dois países. A tecnologia Interledger (https://interledger.org) tem sido avaliada como uma potencial solução para essa questão.

Lightning Network

A Fundação Stellar tem trabalhado para incrementar a rede com a tecnologia *Lightning Network* – solução que garantiria maior escalabilidade e privacidade à rede.[33] A rede *Swipe*, como um *fork* da rede Stellar, pode implementar novas funcionalidades da rede Stellar, adicionando esse e outros potenciais recursos ao protótipo.

33 https://www.stellar.org/blog/lightning-on-stellar-roadmap

Conclusões

As hipóteses levantadas foram validadas por meio de testes experimentais, comprovando, assim, que o protótipo:

- processa transações com um tempo médio de **5,7 segundos** para transações válidas;
- processa transações com um tempo médio de **5,8 segundos** para transações rejeitadas por insuficiência de saldo na conta do PSP;
- é capaz de processar **105 transações por segundo**, mantendo um tempo médio de **9,2 segundos** por transação.

Assim, em uma análise preliminar, o protótipo satisfaz as demandas de rapidez postas como requisitos fundamentais para o sistema de pagamentos instantâneos, e demonstra um nível de escalabilidade proporcional ao recorde de processamento do Sitraf, igual a 5.034.419 TEDs por dia.

Além disso, a demonstração do protótipo por meio de uma carteira digital comprovou ser possível realizar um ecossistema eficiente, competitivo e inclusivo, permitindo tanto transações por meio de intermediários como transações *peer-to-peer*.

Este trabalho deve ser tomado como uma avaliação preliminar do potencial dessa implementação, tanto para o ecossistema de pagamentos instantâneos como para próximas inovações no SFN. Foram levantados diversos assuntos que merecem ser melhor explorados por próximos estudos. Considerando a finalização dos requisitos fundamentais do ecossistema em dezembro de 2018, e a definição das ações necessárias para concretizá-lo sendo definidas a partir de 2019, os autores deste trabalho consideram o momento propício para estudos mais aprofundados.

Referências

ANDROULAKI; BARGER; BORTNIKOV *et al.* **Hyperledger fabric: a distributed operating system for permissioned blockchains**. 2018. Disponível em: https://arxiv.org/pdf/1801.10228.pdf. Acesso em: 23 nov. 2018.

BECH; SHIMIZU; WONG. The quest for speed in payments**. Bank for International Settlements Research & Publications**, 2017. Disponível em: https://www.bis.org/publ/qtrpdf/r_qt1703g.htm. Acesso em: 17 out. 2018.

BURGOS, A. V. et. al. **Distributed ledger technical research in Central Bank of Brazil**. 2017. Disponível em: https://www.bcb.gov.br/htms/novaPaginaSPB/Requisitos%20fundamentais%20-%20vers%C3%A3o%20intermedi%C3%A1ria.pdf. Acesso em: 17 out. 2018.

BANCO CENTRAL DO BRASIL. **Requisitos fundamentais para o ecossistema de pagamentos instantâneos brasileiro (versão intermediária)**. 2018. Disponível em: https://www.bcb.gov.br/htms/novaPaginaSPB/Requisitos%20fundamentais%20-%20vers%C3%A3o%20intermedi%C3%A1ria.pdf. Acesso em: 17 out. 2018.

BANK FOR INTERNATIONAL SETTLEMENTS. **Distributed Ledger Technology in payment, clearing and settlement**. 2017. Disponível em: https://www.bis.org/cpmi/publ/d157.pdf. Acesso em: 17 out. 2018.

BANK FOR INTERNATIONAL SETTLEMENTS. **Fast payments – Enhancing the speed and availability of retail payments**. 2016. Disponível em: https://www.bis.org/cpmi/publ/d154.pdf. Acesso em: 17 out. 2018.

BANK OF CANADA; PAYMENTS CANADA; R3. **Project Jasper:** a Canadian experiment with Distributed Ledger Technology for domestic interbank payments settlement. 2016. Disponível em: https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf. Acesso em: 17 out. 2018.

BANK OF ENGLAND. **FinTech accelerator proof of concept – Ripple**. 2017. Disponível em: https://www.bankofengland.co.uk/-/media/boe/files/fintech/ripple.pdf. Acesso em: 17 out. 2018.

BANK OF ENGLAND. **Fintech proof of concept – Chain**. 2018. Disponível em: https://www.bankofengland.co.uk/-/media/boe/files/fintech/chain.pdf. Acesso em: 17 out. 2018.

BURGOS; BATAVIA. **O meio circulante na era digital**. 2018. Disponível em: https://www.bcb.gov.br/htms/public/inovtec/O-Meio-Circulante-na-Era-Digital.pdf. Acesso em: 23 nov. 2018.

CHASE; MACBROUGH. **Analysis of the XRP Ledger Consensus Protocol**. 2018. Disponível em: https://www.researchgate.net/publication/323302411_Analysis_of_the_XRP_Ledger_Consensus_Protocol. Acesso em: 17 out. 2018.

EUROPEAN CENTRAL BANK; BANK OF JAPAN. **Stellar –** A joint research project of the European Central Bank and the Bank of Japan. 2018. Disponível em: https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf. Acesso em: 17 out. 2018.

FINRA. **Distributed Ledger Technology:** implications of blockchain for the securities industry. 2016. Disponível em: https://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf. Acesso em: 17 out. 2018.

HEARN. **Corda: a distributed ledger**. 2016. Disponível em: https://www.corda.net/content/corda-technical-whitepaper.pdf. Acesso em: 22 nov. 2018.

MONETARY AUTHORITY OF SINGAPORE. **Project Ubin:** SGD on distributed ledger. 2017. Disponível em: http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf. Acesso em: 17 out. 2018.

MONETARY AUTHORITY OF SINGAPORE. **Project Ubin Phase 2:** re-imagining RTGS. 2017. Disponível em: http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20Phase%202%20Reimagining%20RTGS.pdf. Acesso em: 17 out. 2018.

MONETARY AUTHORITY OF SINGAPORE. **Project Ubin:** delivery versus payment on Distributed Ledger Technologies. 2018. Disponível em: http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20DvP%20on%20Distributed%20Ledger%20Technologies.pdf. Acesso em: 20 nov. 2018.

MAZIÈRES. **The Stellar consensus protocol**. 2015. Disponível em: https://www.stellar.org/papers/stellar-consensus-protocol.pdf. Acesso em: 17 out. 2018.

NATARAJAN; KRAUSE; GRADSTEIN. Distributed Ledger Technology (DLT) and blockchain (English). 2017. **FinTech Note**, n. 1. Washington, D.C.: World Bank Group. Disponível em: http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain. Acesso em: 17 out. 2018.

OMFIF; IBM. **Central Bank digital currencies:** a collaboration between OMFIF and IBM blockchain world wire. 2018. Disponível em: https://thinktank.omfif.org/ibm. Acesso em: 8 nov. 2018.

REISS. **CBDC: issues for discussion**. 2018. Disponível em: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/D-Reiss.PDF. Acesso em: 23 nov. 2018.

SCHWARTZ; YOUNGS; BRITTO. **The Ripple protocol consensus algorithm.** 2014. Disponível em: https://ripple.com/files/ripple_consensus_whitepaper.pdf. Acesso em: 17 out. 2018.

SOUTH AFRICAN RESERVE BANK. **Project Khokha:** exploring the use of distributed ledger technology for interbank payments settlement in South Africa. 2018. Disponível em: https://www.resbank.co.za/Lists/News%20and%20Publications/Attachments/8491/SARB_ProjectKhokha%2020180605.pdf. Acesso em: 20 nov. 2018.

Agradecimentos

Este projeto foi elaborado pelos integrantes da *fintech* Swipe. Agradecemos a toda a equipe responsável pela iniciativa do LIFT e pelo apoio: Banco Central do Brasil, Fenasbac, Comitê de Gestão e Coordenação do LIFT, e Grupo de Acompanhamento deste Projeto (GAP).

Swipe
João Paredes
Kalil Reis de Sisto
Ítalo Nascimento
Paulo Pigatto
Vitor Almeida

LIFT-BCB
André Siqueira
Breno Lobo
Marcus Suares
Paulo Caetano da Silva
Rafael Sarres
Ramses Henrique Martinez
e demais membros