LIFT *papers*

Revista do Laboratório
de Inovações Financeiras
e Tecnológicas

#5 | ABRIL 2023

Fenasbac

BANCO CENTRAL
DO BRASIL

LIFT Papers

Revista do Laboratório de Inovações Financeiras e Tecnológicas

Número 5 | Abril 2023

Ficha catalográfica elaborada pela Biblioteca do Banco Central do Brasil

LIFT Papers / Banco Central do Brasil. N. 5, (abril 2023). Brasília: Banco Central do Brasil, 2020.

Semestral
Disponível em:
https://revista.liftlab.com.br
ISSN 2675-2859

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

CDU 336.7:004.738.5(05)

Interoperabilidade entre o Real Digital e um Blockchain público

Edmilson Rodrigues do Nascimento Junior[1]
Juliandson Estanislau Ferreira[2]

Propiciar a interoperabilidade do Real Digital com *blockchains* públicos ou privados é essencial para contribuir para um Sistema Financeiro nacional aberto, inclusivo, seguro e competitivo. O presente trabalho faz uma análise de conceitos ligados a *blockchains* e interoperabilidade, bem como propõe um caso de uso e executa uma prova de conceito em que investidores internacionais podem adquirir um ativo tokenizado na *ledger* do Real Digital usando *stablecoin* em um *blockchain* público. A tokenização de ativos da economia real (*Real World Assets* – RWA) irá revolucionar essa indústria e permitir que o ciclo de investimento e desinvestimento nesses ativos seja feito de forma atômica, programática e em minutos ao invés de dias, reduzindo a burocracia e melhorando o tempo de execução. O método usado para a interoperabilidade foi o de integração direta usando *Hashed Time Locked Contracts* em ambos os *blockchains*. Superando-se os desafios tecnológicos, o artigo também menciona possíveis restrições à interoperabilidade, que são a regulamentação e o problema dos oráculos na *ledger* do Real Digital. Promover a interoperabilidade do Real Digital é essencial para que todos os brasileiros possam se beneficiar de menor custo de serviços financeiros, maior competitividade entre *players*, maior inclusão de usuários de baixa renda e maior sustentabilidade, contribuindo, assim, para vários fatores da Agenda BC#.

Palavras-chaves: CBDC; real digital; *blockchain*; interoperabilidade; pagamentos.

1 MsC (CIn/UFPE) - ernj@cin.ufpe.b
2 MsC (Cin/UFPE) - jef@cin.ufpe.br

Introdução

Com o advento do Real Digital, que dará habilidades à moeda brasileira como programabilidade e composabilidade, é importante também promover a interoperabilidade entre a CBDC brasileira e *blockchains* públicos, como o Bitcoin, Ethereum, Celo e outros, para que pessoas e organizações que são criptonativas possam investir na economia brasileira, beneficiando, assim, o Sistema Financeiro Nacional. Este projeto examina como as moedas digitais do Banco Central (CBDCs) podem contribuir para um sistema monetário aberto, seguro e competitivo que apoie a inovação e atenda ao interesse público. Além disso, explora aspectos importantes relacionados à interoperabilidade entre o Real Digital e um *blockchain* público, destacando os principais benefícios dessa interoperabilidade.

Analisamos também como as tecnologias *blockchain* e os contratos inteligentes podem ser utilizados para a construção de aplicações que possam ajudar os bancos centrais a criarem suas CBDCs e quais os principais desafios a serem superados. Destacamos como a tecnologia poderá impactar o processo de compra, venda e gerenciamento de títulos da dívida pública brasileira e outros ativos financeiros.

Este artigo está organizado em oito capítulos, os quais são detalhados a seguir: no capítulo 1, fornecemos uma visão geral dos objetivos do projeto. No capítulo 2, apresentamos uma revisão de literatura investigando os conceitos relacionados a *blockchain*, contratos inteligentes, tokenização e interoperabilidade. Todos os conceitos explorados compõem a base conceitual para o desenvolvimento do projeto proposto. O capítulo 3 descreve a visão geral do projeto destacando suas características gerais e seus mecanismos de funcionamento. No capítulo 4, apresentamos as principais funcionalidades do protótipo, explicando as características de cada um de seus elementos. No capítulo 5, delimitamos o escopo geral do projeto. No capítulo 6, são destacadas as características inovadoras. No capítulo 7, são apresentados os resultados teóricos e práticos obtidos com a realização da presente pesquisa, destacando as principais contribuições para o Sistema Financeiro Nacional. No capítulo 8, discutimos as principais restrições legais e tecnológicas para a implantação do projeto. Por fim, apresentamos as considerações finais sobre o trabalho.

1 Objetivos

O presente projeto do LIFT Lab tem o objetivo de estudar a interoperabilidade entre a *ledger* do Real Digital, que será representada durante o LIFT Lab 2022 por uma rede *blockchain testnet* criada na ferramenta *Geth*[3], que tem as características de ser permissionada e baseada na *ethereum virtual machine* (EVM), e o *blockchain* público da Celo. A Celo foi escolhida por ter custos de transação e tempo de conclusão das transações muito baixos.

Dessa forma, usando o protótipo que iremos construir, indivíduos poderão fazer transações de *blockchains* públicos para a *ledger* do Real Digital de forma atômica e programática, reduzindo custos e aumentando a eficiência. A interoperabilidade entre a *ledger* do Real Digital e *blockchains* públicos irá permitir que pessoas ou organizações que são criptonativas possam adquirir ativos da economia real, contribuindo, assim, para o aumento da concorrência, a redução de custos de serviços de conversão e de maior disponibilidade de capital para o Sistema Financeiro Nacional, objetivos que estão alinhados com a Agenda BC#.

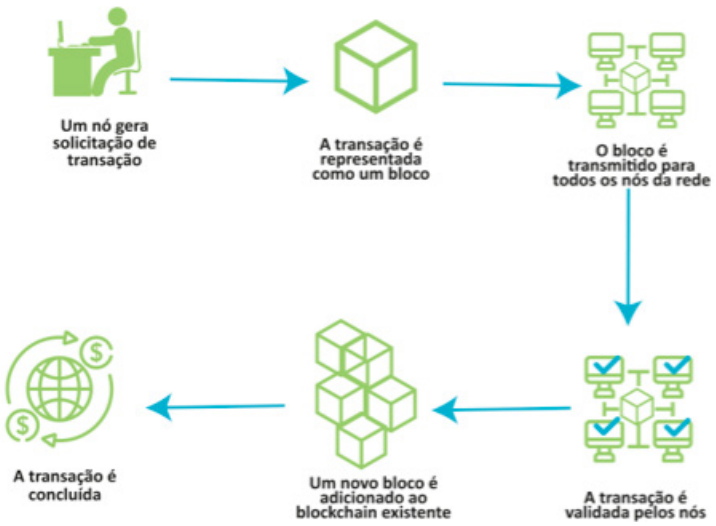
3 Disponível em: https://geth.ethereum.org/.

2 Fundamentação Teórica

2.1 Blockchain

Blockchain é um *ledger* (livro-razão) distribuído, on-line, público, imutável, que é compartilhado por meio de uma rede de computadores *peer-to-peer* (P2P) e pode ser atualizado por qualquer nó participante. Além disso, todos os nós mantêm uma cópia do *ledger* contendo cada transação desde o início da rede (CASINO; DASAKLIS; PATSAKIS, 2019). A figura 1 ilustra o processo de inclusão de transações da rede *blockchain*. Qualquer transação a ser incluída deve ser primeiramente autorizada pela assinatura digital do proprietário. O principal dessa etapa é autenticar a transação e protegê-la contra adulterações, o que garantirá a segurança do sistema.

Figura 1. Estrutura das transações *blockchain*



Fonte: Casino, Dasaklis, & Patsakis, 2019.

As transações são transmitidas a todos nós validadores que participam da rede, que normalmente competem entre si para validá-las da forma mais eficiente e eficaz possível. Ao fim do processo de validação das transações, será um novo bloco candidato a ser adicionado ao *blockchain*. Para isso, é necessário primeiro haver um acordo entre os validadores, o que, normalmente, é atingido por um algoritmo específico consenso. Dentre eles, os que mais se destacam são: *proof-of-work* e *proof-of-stake*. Tais algoritmos de consenso também têm o objetivo de dissuadir ataques cibernéticos (KYPRIOTAKI; ZAMANI; GIAGLIS, 2015), visto que, para qualquer atacante adulterar os dados, é necessário possuir 51% de poder de processamento da rede. Uma vez que as transações são verificadas e aceitas como verdadeiras por toda a rede, os validadores começam a trabalhar no próximo bloco. Como cada transação é registrada de forma transparente e compartilhada entre todos os validadores, é aberta para qualquer pessoa ver.

O conceito do *blockchain* foi apresentado ao mundo em 2009 por meio da publicação do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System* por um indivíduo com o pseudônimo de Satoshi Nakamoto como alternativa à abordagem centralizada e baseada na confiança. Um dos principais benefícios da tecnologia *blockchain* baseia-se no fato de que, apesar de ter sido inicialmente apresentada como uma solução de problemas específicos relacionados

à indústria de serviços financeiros, pode ser adaptada a qualquer setor em que seja necessário registrar, confirmar e transferir qualquer tipo de contrato ou propriedade. As características mais relevantes dos *ledgers* distribuídos incluem (WÜST; GERVAIS, 2018):

- **Descentralização**: essa é uma propriedade fundamental, pois não há autoridade central proprietária dos dados; em vez disso, os dados são distribuídos entre os nós da rede (daí o nome "*ledger* distribuído"), e nenhum deles sozinho pode influenciar ou manipular a rede.

- **Transparência**: uma das principais características do *blockchain* é sua transparência. Isso significa que o registro de transações é totalmente rastreável, auditável, preciso e muito mais fácil de manter, apesar da tecnologia permitir transações anônimas.

- **Imutabilidade**: se alguém tentar alterar a transação na rede, todos os blocos subsequentes terão que ser alterados. Essa propriedade torna praticamente impossível para qualquer entidade manipular, substituir ou falsificar dados armazenados na rede.

A tecnologia *blockchain* representa grande avanço na manutenção de registros e transações que são registrados e verificados por uma rede em vez de uma única autoridade central. A tecnologia foi proposta para lidar com as ineficiências típicas de sistemas centralizados. Esses tipos de sistemas normalmente possuem gargalos e dificultam acordos de transação. Os *ledgers* distribuídos podem ser classificados em *permissionless* ou *permissioned*, a depender das seguintes características:

- **Permissionless**: são redes tipicamente abertas e descentralizadas. O *blockchain* não possui um dono específico e permite que qualquer pessoa que queira participar da rede tenha uma cópia idêntica dos dados e permissão para modificá-los. No entanto, uma única entidade sozinha não pode desligar a rede ou alterar seus protocolos. Para que uma nova transação seja inserida, será necessária a concordância de mais de 50% dos validadores. Nenhum validador pode impedir que transações sejam adicionadas e, uma vez inseridas, não podem ser editadas.

- **Permissioned**: são redes fechadas nas quais partes previamente designadas, às vezes membros de um consórcio, interagem e participam do consenso. Esse tipo de *blockchain* só pode ser acessado por usuários que foram expressamente autorizados pelo administrador. Normalmente, os usuários recebem diferentes tipos de privilégios de acordo com as ações que pretendem realizar. Embora não exista qualquer autoridade central, permite que um grupo privado verifique a integridade de seus dados, o que torna todo processo de verificação bem mais simples. Essa solução tem se mostrado bastante efetiva, já que eles são mais rápidos e escaláveis que os *permission less blockchains*.

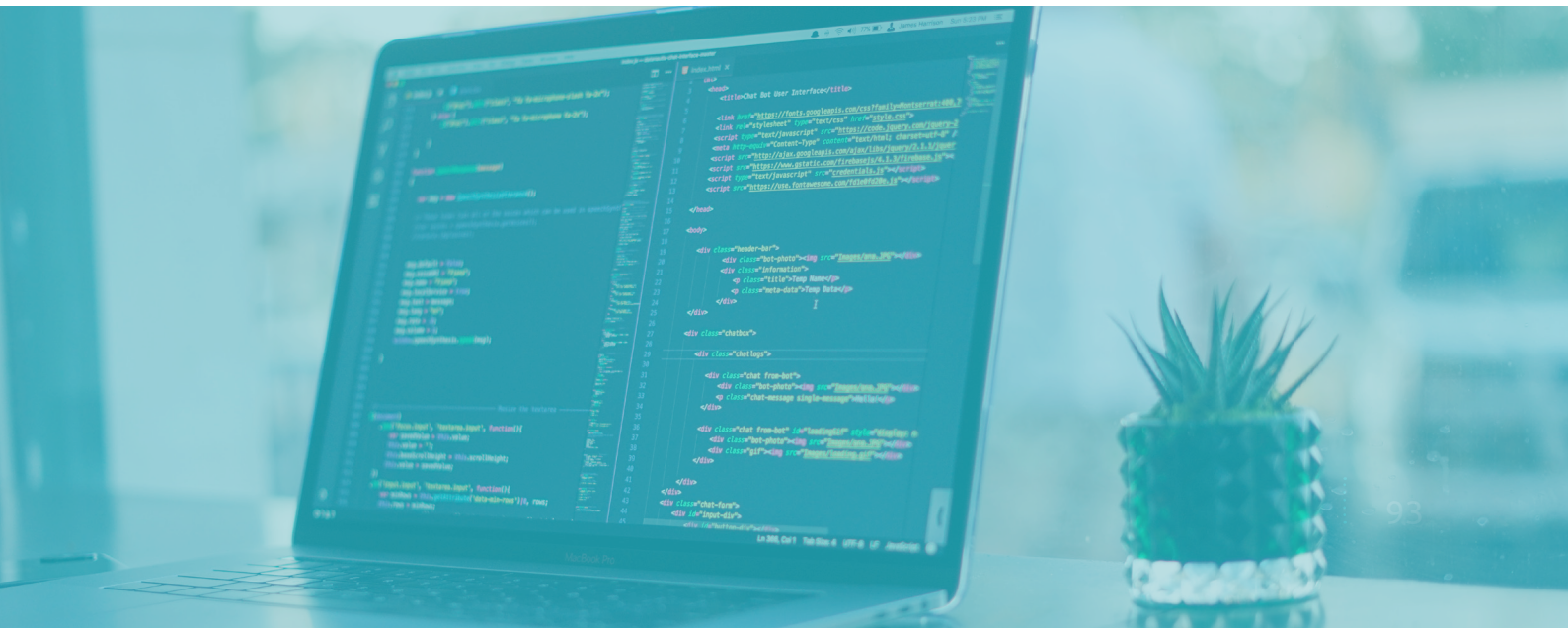
A grande novidade do *blockchain* está no fato de que ele é mais que um banco de dados; é possível também definir regras de negócio que estão diretamente ligadas às suas transações. Portanto, seu verdadeiro potencial só é aproveitado quando combinado com *smart contracts*. Nesse sentido, já surgiram várias ideias inovadoras que aproveitam o melhor das duas tecnologias. Podem-se criar aplicações de registros públicos descentralizados, como títulos de terra, emissão de passaportes, votação e antecedentes criminais, ou registros privados, como testamentos e *trusts*. Desde o seu surgimento, o interesse pela tecnologia *blockchain* cresceu significativamente, sendo considerada hoje por muitos especialistas como uma tecnologia de alto grau inovador, visto que possui o potencial para impactar profundamente a forma como a sociedade se organiza.

2.2 Contratos Inteligentes

À medida que o *blockchain* se desenvolveu, foi incluída a capacidade de executar contratos inteligentes, que se tornou fundamental para construir aplicações mais complexas. Contrato inteligente é um termo usado para descrever um programa de computador, armazenado no *blockchain*, capaz de facilitar transações entre duas ou mais partes anônimas sem a necessidade de um intermediário. Além disso, por meio desse mecanismo é possível fazer com que se cumpram as cláusulas previstas no contrato, parcialmente ou em sua totalidade, quando condições predeterminadas são atendidas. Todo o processo é automático e pode ser utilizado com complemento de contratos legais, ou até mesmo substituí-los. Os termos do contrato seriam escritos como um conjunto de instruções e executados sem a necessidade de uma entidade reguladora (SZABO, 2016). O conceito de contratos inteligentes foi criado em meados dos anos 1990 por Nick Szabo, que também foi um dos idealizadores do Bit Gold. Uma moeda digital que nunca chegou a ser implementada, mas foi a precursora da *bitcoin*, visto que possuía várias características em comum: estrutura descentralizada, foco na privacidade e uso de criptografia.

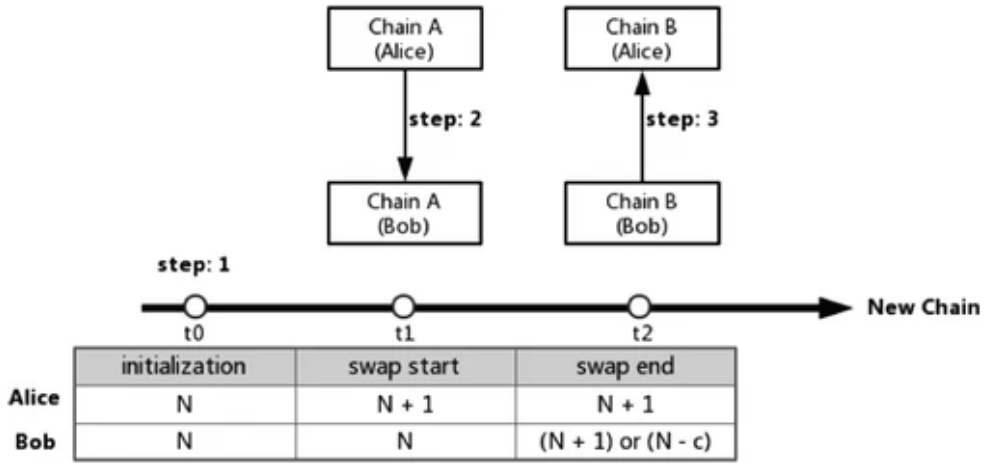
Embora os contratos inteligentes possam funcionar em ecossistemas financeiros tradicionais somente quando associados ao *blockchain*, todo o seu potencial pode ser explorado. O fato de eles serem digitais e automatizados elimina a burocracia e evita erros humanos durante o processo. As cláusulas dos contratos inteligentes podem ser acessadas por qualquer participante da rede, o que torna o sistema mais transparente e confiável, pois há menos margem para interpretações dúbias e disputas. Os registros de transações são compartilhados com vários nós e evitam-se problemas típicos de sistemas centralizados, como: gargalos na rede e criação de um único ponto de falha. Além disso, os contratos inteligentes são extremamente difíceis de *hackear* por serem criptografados, e seus termos são executados assim que as condições das cláusulas são satisfeitas, o que reduz o tempo gasto em uma negociação tradicional.

Uma das aplicações possíveis para contratos inteligentes é para facilitar a troca de *tokens* entre *blockchains*, ou seja, contratos "*cross-chain*". Entre os contratos *cross-chain,* há aqueles que são "atômicos". Em outras palavras, que têm apenas dois resultados possíveis, 0 ou 1, ou a troca de ativos acontece e ambos os participantes recebem os ativos trocados ou não acontece e ambos recebem os ativos originais. O método usado neste estudo e que é um dos mais mencionados pela literatura para a troca *cross-chain* de forma atômica é o *"Hashed Time Locked Contracts (HTLC)"* (RUEEGGER; MACHADO, 2020). O método HTLC consiste em ambos os participantes (Alice e Bob) terem ativos diferentes e desejarem fazer



uma troca (t0). Então, Alice envia o *token* para o *smart contract* em t1. Os contratos são protegidos pelo *hash* de um número gerado randomicamente (daí o termo *hashed*) e têm um prazo máximo para expirarem (daí o termo "*time locked*"). Então, só existem dois resultados possíveis em t2: ou Bob também envia seu *token* para o *smart contract* e Alice libera o *hash* para liberar o seu *token* para Bob, ou Bob não envia o *token* para o contrato, o tempo expira e Alice recebe de volta os seus *tokens* no endereço de origem.

Figura 2. Funcionamento do HTLC



	initialization	swap start	swap end
Alice	N	N + 1	N + 1
Bob	N	N	(N + 1) or (N - c)

Fonte: Rueegger e Machado, 2020.

2.3 Tokenização

Tokenização é o processo de representação digital de um ativo real em um *blockchain* (HILEMAN; RAUCHS, 2017). O processo de tokenização busca minimizar a quantidade de dados que uma empresa precisa manter para realizar suas transações (LUTKEVICH, 2021) e pode oferecer ampla gama de benefícios, como custos de transação mais baixos, maior transparência, liquidez, eficiência, acesso a fontes alternativas de capital e descentralização. Apesar da diversidade de *tokens*, a maioria deles pode ser generalizada em três categorias:

- ***Fungible tokens*:** são divisíveis e não podem ser distinguidos uns dos outros pela análise de suas propriedades. Esta é a categoria mais simples de *tokens*, e os casos de uso básicos são bastante diretos. O mais comum são as criptomoedas. ERC20 é o padrão mais básico e mais adotado para representação desse tipo de *token*.

- ***Non-fungible tokens*:** são usados para ativos que exigem uma identificação digital exclusiva. Normalmente são representados pelo padrão ERC721. Por meio desse tipo de *token* é possível registrar, verificar e rastrear a propriedade de um ativo exclusivo. Os NFTs podem ser utilizados para representar qualquer tipo de objeto que possa ser considerado único ou raro como: obras de arte, contratos futuros, imóveis etc.

- ***Hybrid tokens*:** os tokens híbridos são uma mistura de ambos. Ao combinar as vantagens de fungibilidade e não fungibilidade, os *tokens* híbridos geralmente aparecem como uma maneira relevante de representar ativos financeiros. O padrão ERC1400 é um dos mais utilizados para o caso de uso de ativos financeiros tokenizados. É compatível com ERC20 e, ao mesmo tempo, permite representar diferentes classes de ativos.

2.4 Interoperabilidade

Em se tratando de sistemas de *blockchain*, a interoperabilidade é definida pela *European Blockchain Observatory* como "a habilidade de trocar dados com outras plataformas, incluindo outros tipos de blockchain e com o mundo Off-chain" (EU BLOCKCHAIN, 2019, p. 5). Promover a interoperabilidade é importante, pois estimula a competição, reduz custos, permite a economia de escala e aumenta a conveniência aos usuários. Embora a interoperabilidade seja um tema de extrema relevância, a maioria das aplicações não conseguiram se beneficiar totalmente da tecnologia *blockchain* devido à incapacidade de vários *blockchains* se comunicarem, fato esse que impacta significativamente a experiência do usuário.

Existem várias formas de se fazer a interoperabilidade entre *blockchains*. Pillai *et al.* (2022) apresentam *framework* para processo decisório sobre qual o melhor desenho para a interoperabilidade. O *framework* consiste em cinco passos, quais sejam: (i) identificar o tipo de valor/ativo que será usado na aplicação; (ii) identificar o objetivo da integração; (iii) selecionar a abordagem, se centralizada ou descentralizada; (iv) escolher o modo de integração; e (v) escolher o protocolo de integração.

Em se tratando de interoperabilidade entre *Central Bank Digital Currencies* (CBDCs), o *Bank of International Settlements* (BIS) está desenvolvendo, em parceria com várias instituições, o projeto *mBridge*. Trata-se de uma colaboração entre o *BIS Innovation Hub*, de Hong Kong, e outros parceiros que colaboraram para a criação de uma nova arquitetura de *blockchain*, a *mBridge Ledger*, que serve como plataforma especializada e flexível para que bancos centrais possam implementar pagamentos transfronteiriços entre CBDCs. A iniciativa está em fase de piloto e, ao longo de testes conduzidos em 2022, 20 bancos comerciais em quatro jurisdições transacionaram USD$22 milhões em valor.

2.5 Oráculos

Em sistemas de *blockchains*, oráculos são infraestruturas tecnológicas providas por partes centralizadas e confiáveis para serem a interface entre os programas que rodam nos *blockchains* e o "mundo real". Por exemplo, dados como cotação entre moedas, temperatura de ambientes, cotação de ações, eventos em outros *blockchains* e outras informações são normalmente providos por oráculos (CALDARELLI, 2020).

A literatura acadêmica e o histórico dos *blockchains* públicos mostram que é possível ocorrer problemas associados aos oráculos, levando a falhas de segurança para os *smart contracts* ou a impossibilidade de execução dos projetos. Alguns dos riscos associados aos problemas dos oráculos são: (i) risco de segurança da informação (informações imprecisas ou falsas); (ii) risco de baixa latência (atualização) dos dados; (iii) risco de comprometimento da reputação da entidade que mantém o oráculo, entre outros (CALDARELLI, 2020).

Por causa desse papel importante para a execução de *smart contracts*, os oráculos são parte fundamental para a infraestrutura tecnológica e já têm de estar disponível com o lançamento do Real Digital.

3 Visão Geral

Para fins do estudo, escolhemos o caso de uso da compra e venda de títulos da dívida brasileira. Isso porque o advento do Real Digital e sua *ledger*, que dará uma camada de inteligência para o Sistema Financeiro Nacional, permitirá também a tokenização de ativos da economia real, também conhecidos como *Real World Assets* (RWA).

Hoje em dia, o processo de investimento no Tesouro Direto é controlado por três atores: (i) Cetip; (ii) B3; e (iii) bancos e/ou as corretoras. A (i) Cetip é a integradora do mercado financeiro e faz o registro, a custódia e a liquidação dos títulos; a (ii) B3 faz o cadastro de investidores e o fracionamento dos títulos em frações de 1.000 para que investidores possam aportar a partir de R$ 30; e os (iii) bancos e as corretoras fazem a distribuição desses títulos fracionados para os investidores pessoa física.

Ao tokenizar os títulos da dívida brasileira e permitirmos que eles sejam comprados de forma programática entre *blockchains*, contribuiremos para dar acesso a novos investidores para a eficiência dos processos envolvidos na emissão, custódia e liquidação dos títulos e para a democratização dos retornos dessa modalidade de investimento, que são pontos da Agenda BC#.

Em adição, ao permitir que os *tokens* do Título da Dívida Brasileira sejam adquiridos por meio de *stablecoin* da rede Celo, estaremos testando a interoperabilidade do *ledger* do *blockchain* do Real Digital com a de um *blockchain* público que roda a EVM. No protótipo a ser desenvolvido durante o LIFT Lab, o usuário deve permitir comprar e vender um *token* que representa o título da dívida brasileira usando uma *stablecoin* da Celo atrelada ao real brasileiro, a cREAL.

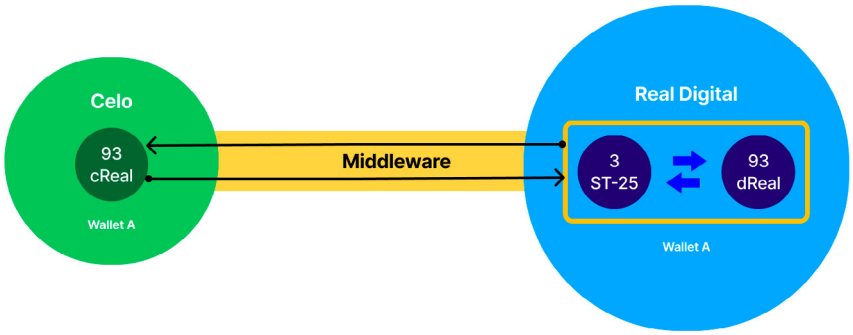
4 Funcionalidades

De modo simplificado, para comprar ou vender um título do Tesouro Tokenizado, o usuário: (i) faz o *login* conectando sua carteira Celo Web3 (Ex.: Metamask); (ii) caso seja a primeira vez, faz o KYC (abstraído da prova de conceito); (iii) escolhe o título e o valor a ser investido; (iv) faz a troca da *stablecoin* cREAL (padrão ERC-20) na rede Celo para o seu título da dívida de preferência; (v) recebe de volta na mesma carteira na *ledger* do Real Digital o título (*token* "ST25 – *Simple Token* Tesouro vencimento em 2025"); (vi) quando quiser vender sua posição, faz o caminho oposto e receberá de volta o valor em *stablecoin* na Celo.

5 Escopo do Protótipo no LIFT

O protótipo a ser construído durante o LIFT Lab 2022 visa testar o caso de uso da interoperabilidade entre um *blockchain* público que roda EVM (o da Celo) e um que representará o do Real Digital. Dessa forma, iremos focar apenas na (i) troca de *tokens* da *ledger* do Real Digital para o *blockchain* da Celo, e vice-versa. Para fins do escopo do protótipo, também transacionaremos somente o *token* ERC20 cREAL e, para fins de simplificação, ele sempre terá paridade 1 para 1 com o Real Digital.

Figura 3. Escopo do protótipo do LIFT Lab



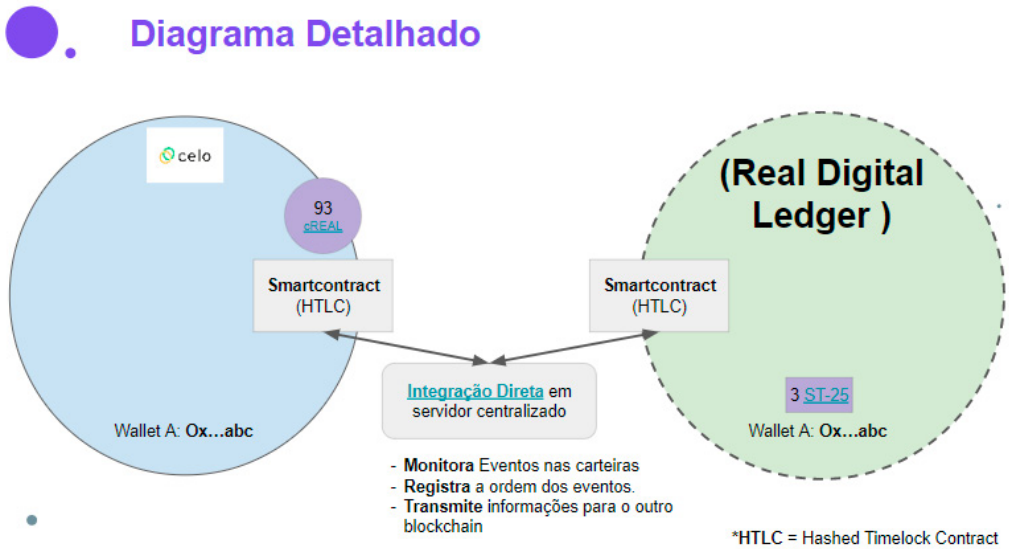
Fonte: Elaboração própria (2022).

Também para fins de simplificação, o (ii) *token* que representa o título da dívida brasileira, o *Simple Token* Tesouro (ST-25), já estará criado na *ledger* que representa o Real Digital.

Sendo assim, a equipe do projeto considera que testar a interoperabilidade é executar com qualidade a funcionalidade 1. O processo de tokenização do título da dívida brasileira na *ledger* do Real Digital foi abstraído dessa prova de conceito por causa da restrição de tempo.

Seguindo o *framework* para a escolha do desenho da interoperabilidade de Pillai *et al.* (2022), a prova de conceito apresenta as seguintes características: (i) transfere criptoativos; (ii) tem o objetivo de fazer a troca entre criptoativos; (iii) tem abordagem centralizada; (iv) possui modo de integração via *Hashed TimeLocked Contracts*; e (v) possui protocolo de integração tipo *lock/unlock*.

Figura 4. Diagrama detalhado do protótipo do LIFT Lab



Fonte: Elaboração própria (2022).

Por conseguinte, a prova de conceito de interoperabilidade no Real Digital funciona ao permitir que, com o mesmo par de chaves pública e privada nos dois *blockchains* que rodam a EVM:

1. por meio da interface, o usuário faz a troca de cREAL pelo Simples Tesouro Tokenizado (*token* ST). O que, na prática, consiste em enviar o cREAL para o *smart contract* com o mecanismo de *Hashed Time Locked Contract* na rede da Celo;
2. a informação é captada pela aplicação da integração direta que fica no servidor centralizado;
3. a mensagem contendo a carteira de origem, o valor enviado e o título comprado é registrada no log da integração direta no servidor centralizado;
4. o mecanismo da integração direta envia a mensagem contendo o título comprado e a carteira de destino, mas no *blockchain* que representa o Real Digital.
5. o *Hashed Timelocked Contract* na rede do Real Digital envia o título do Tesouro Tokenizado (ST-25) para a carteira de destino;
6. caso queira liquidar o título adquirido, o usuário faz o caminho inverso: por meio da interface, troca o Simples Tesouro Tokenizado por cREAL.

6 Características Inovadoras

Hoje em dia, o processo de investimento no Tesouro Direto é controlado por três atores: (i) Cetip; (ii) B3; e (iii) Bancos e/ou corretoras. A (i) Cetip é a integradora do mercado financeiro e faz o registro, a custódia e a liquidação dos títulos; a (ii) B3 faz o cadastro de investidores e o fracionamento dos títulos em frações de 1.000 para que investidores possam aportar a partir de R$ 30; e os (iii) bancos e as corretoras fazem a distribuição desses títulos fracionados para os investidores pessoa física.

A tokenização de títulos da dívida pública e outros ativos da economia real (Real World Assets – RWA) irá revolucionar essa indústria e permitir que o ciclo de investimento e desinvestimento em ativos da economia real como os títulos do Tesouro Brasileiro seja feito de forma atômica, programática e em minutos, ao invés de dias. Reduzirá a burocracia, melhorando o tempo de execução e fazendo com que o registro, a custódia e a liquidação dos valores sejam feitos na *ledger* do Real Digital e auditados *pós-facto* pela Cetip e B3. As ordens de compra e venda serão registradas na *ledger* do Real Digital por bancos ou corretoras, mas podem ser iniciadas pelos próprios donos das chaves públicas/privadas, dando ao usuário, se assim o desejar, a capacidade de autocustódia dos *tokens*.

A principal característica inovadora da promoção da interoperabilidade de *blockchains* públicos com a *ledger* do Real Digital consiste no fato de que dará mais visibilidade aos ativos da economia brasileira e permitirá que investidores de qualquer lugar do mundo que são criptonativos aportem seu capital no Sistema Financeiro Nacional, aumentando, dessa forma, a conveniência aos usuários e a oferta de capital para ativos da economia brasileira.

7 Contribuição para o Sistema Financeiro Nacional

A infraestrutura para interoperabilidade entre o Real Digital e *blockchains* públicos que rodam a EVM desenvolvida pela *Lovecrypto* nessa prova de conceito pode ser útil não só para a negociação de títulos da dívida brasileira, mas para qualquer *token*/ativo registrado na *ledger* do Real Digital.

Pessoas e organizações de qualquer lugar do mundo que são criptonativas (mantêm a maior parte de seus recursos em criptomoedas) poderão investir em títulos da dívida brasileira e outros ativos tokenizados na *ledger* do Real Digital. Isso dará visibilidade aos ativos da economia brasileira e permitirá que maior quantidade de recursos fique disponível para investimento no Sistema Financeiro Nacional, além de aumentar a conveniência a usuários que são criptonativos.

Ao permitir a interação de forma atômica e programática de aplicações descentralizadas (dApps) de *blockchains* públicos com a ledger do Real Digital, também podemos pensar no surgimento de casos de uso de aplicações *cross-chain*, que se iniciam em *blockchains* públicos, executam-se na *ledger* do Real Digital, ou vice-versa.

Dessa forma, ao unir os mundos dos *blockchains* públicos (a internet do valor) com o mundo do Real Digital, iremos contribuir para a inclusão, competitividade e sustentabilidade do Sistema Financeiro Nacional, ideais presentes na Agenda BC#.

8 Restrições

Após quebradas as barreiras tecnológicas da interoperabilidade entre as *ledgers* que rodam a EVM e a *ledger* do Real Digital, e superados os possíveis problemas de segurança da informação, é necessário pensar em possíveis impedimentos que podem surgir para a adoção do uso da tecnologia no mundo real.

Um dos impedimentos é a regulação. Segundo pesquisas preliminares, com a legislação atual, para tokenizar ativos na *ledger* do Real Digital é necessário ser uma securitizadora. Para distribuir ativos tokenizados na *ledger* do Real Digital é necessário ser uma corretora. Portanto, faz mais sentido para a *Lovecrypto* como uma empresa de inovação especializada na tecnologia do *blockchain* se associar com *players* que já tenham essas licenças e se especializar em prover a tecnologia para a interoperabilidade do valor.

Um segundo impedimento será o problema dos oráculos. Em *blockchains*, oráculos são parte da infraestrutura que fazem o *input* de dados do mundo *off-chain* para a *ledger*. Serão necessários oráculos seguros, de baixa latência e resilientes para servir o Sistema Financeiro Nacional com informações como cotação entre moedas, taxa Selic, IPCA, entre outros indicadores, a fim de que os *smart contracts* da aplicação que envisionamos possam funcionar com qualidade.

Um terceiro impedimento advém do fato de que, por restrição de tempo durante o desafio do LIFT Lab 2022, a equipe escolheu um desenho centralizado e de integração direta para a interoperabilidade do *blockchain* público com o do Real Digital. No entanto, pessoas que são criptonativas tendem a preferir desenhos que são descentralizados e "*trustless*", ou seja, que não têm um ponto de falha único, pois têm muitas redundâncias em sua arquitetura e, por isso, não depositam a confiança em nenhuma entidade em particular. Para ter uma arquitetura descentralizada e "*trustless*", é necessário repensar a aplicação de interoperabilidade, o que pode ser feito na fase de piloto, no ano de 2023, se a *Lovecrypto* for escolhida para tal fase.

Conclusão

Alguns autores, como Tapscott e Tapscott (2018), afirmam que, graças à tecnologia do blockchain, estamos entrando em uma nova fase da internet, a internet do valor. Para que o Real Digital tenha a penetração e o impacto que a internet da informação tem hoje na vida dos brasileiros, um dos problemas que o Real Digital e o Sistema Financeiro Nacional vão ter que resolver é o da interoperabilidade com os *blockchains* públicos e com outras CBDCs.

Ao fazer com que as diversas *ledgers*, tanto públicas como governamentais, sejam interoperáveis de forma fluida e com baixo custo, os brasileiros poderão colher os benefícios de menor custo por serviços, maior competitividade entre os *players* e maior inclusão dos clientes de baixa renda. Portanto, a interoperabilidade contribuirá com vários fatores da Agenda BC# ao mesmo tempo.

O presente projeto de interoperabilidade já contribui para a construção de um exemplo de *middleware* para conectar a *ledger* do Real Digital com um *blockchain* público que roda a EVM. O protótipo inicial é limitado a uma única funcionalidade: investimento e desinvestimento de *tokens* que representam um título do tesouro por meio de uma *stablecoin*. Porém, o seu desenho vai permitir melhorias futuras que permitirão expandir suas funcionalidades, por exemplo a compra de outros títulos tokenizados ou a troca de *stablecoins* em diversas redes por Real Digital.

O futuro das finanças passa pela sua convergência com a tecnologia *blockchain*. Ao contribuir para resolver o problema da interoperabilidade, o presente projeto espera contribuir para o Sistema Financeiro Nacional.

Referências

BANCO CENTRAL DO BRASIL – BCB. **Agenda BC#**. 2019. Disponível em: https://www.bcb.gov.br/en/about/bcbhashtag . Acesso em: 9 out. 2022.

BANK OF INTERNATIONAL SETTLEMENTS – BIS. **Project mBridge**: Connecting economies through CBDC. 2022. Disponível em: https://www.bis.org/publ/othp59.htm. Acesso em: 2 nov. 2022.

CALDARELLI, G. Understanding the Blockchain Oracle Problem: A Call for Action. **Information** v. 11, n. 11, p. 1-19, 2020. Disponível em: https://doi.org/10.3390/info11110509.

CASINO, F.; DASAKLIS, T. K.; PATSAKIS, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. **Elsevier**, v. 36, p. 55-81, 2019.

EUROPEAN BLOCKCHAIN OBSERVATORY AND FORUM – EU BLOCKCHAIN. **Scalability, Interoperability and Sustainability of Blockchains**: a Thematic Report. [*S./l.*]: European Comission, 2019. Disponível em: https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pdf. Acesso em: 8 out. 2022.

GO ETHEREUM. **Go Ethereum**: Official Go implementation of the Ethereum protocol. https://geth.ethereum.org/. [*S./d.*]. Acesso em: 5 dez. 2022.

HILEMAN, G.; RAUCHS, M. **Global Blockchain Benchmarking Study**. 2017. Disponível em: http://dx.doi.org/10.2139/ssrn.3040224. Acesso em: 1º out. 2022.

KYPRIOTAKI, K.; ZAMANI, E.; GIAGLIS, G. From bitcoin to decentralized autonomous corporations: Extending the application scope of decentralized peer-to-peer networks and blockchains. *In*: INTERNATIONAL CONFERENCE ON ENTERPRISE INFORMATION SYSTEMS, 17., 2015, Barcelona. **Proceedings [...]**. Setubal: Scitepress, 2015.

LUTKEVICH, B. **Tokenization**. 2021. Disponível em: https://www.techtarget.com/

searchsecurity/definition/tokenization. Acesso em: 1º out. 2022.

PILLAI, B.; BISWAS, K.; HÓU, Z.; MUTHUKKUMARASAMY, V. Cross-Blockchain Technology: Integration Framework and Security Assumptions. **IEEE Access**, v. 10, p. 41239-41259, 2022. doi: 10.1109/ACCESS.2022.3167172.

RUEEGGER, J.; MACHADO, G. S. Rational Exchange: Incentives in Atomic Cross Chain Swaps. *In*: INTERNATIONAL CONFERENCE ON BLOCKCHAIN AND CRYPTOCURRENCY – ICBC, Toronto, 2020, **Paper [...]**. Toronto: IEEE, 2020. Disponível em: doi: 10.1109/ICBC48266.2020.9169408.

SZABO, N. **Smart contracts described by Nick Szabo 20 years ago now becoming reality**. 2016. Disponível em: https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-

szabo-years-ago-now-becoming-reality-1461693751. Acesso em: 1º out. 2022.

TAPSCOTT, D.; TAPSCOTT, A. **Blockchain Revolution**: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World. New York: Penguin Publishing Group, 2018.

WÜST, K.; GERVAIS, A. Do you Need a Blockchain? *In*: CRYPTO VALLEY CONFERENCE ON BLOCKCHAIN TECHNOLOGY, Zug, 2018. **Anais [...]**. Zug: CVCBT, 2018. Disponível em: doi: 10.1109/CVCBT.2018.00011.