



Universidade de Brasília

Faculdade de Direito

Sigilo bancário e direito de privacidade no DREX

Fábio Luis Mendes

Brasília (DF)

2024

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

Sigilo bancário e direito de privacidade no DREX

Autor: Fabio Luis Mendes

Orientador: Daniela Marques de Moraes

Co-Orientador: Gabriel Boavista Laender

Monografia apresentada como requisito parcial para a obtenção do título de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Brasília 2024

FOLHA DE APROVAÇÃO

FABIO LUIS MENDES

Sigilo bancário e direito de privacidade no DREX

Monografia apresentada como requisito parcial para a obtenção do título de Bacharel, no Programa de Graduação da Faculdade de Direito da Universidade de Brasília.

Aprovada em:

BANCA EXAMINADORA

Profª. Dra. Daniela Marques de Moraes

(Orientadora - Presidente)

Prof. Dr. Gabriel Boavista Laender

(Co-Orientador - Membro)

Prof. Dr. Guilherme Pereira Pinheiro

(Membro)

Prof. Dr. (Suplente)

FICHA CATALOGRÁFICA

MF119ss Mendes, Fabio Luis
Sigilo bancário e direito de privacidade no DREX / Fabio Luis Mendes; orientador Gabriel Boavista Laender. -- Brasília, 2024.
50 p.

Monografia (Graduação - Direito) -- Universidade de Brasília, 2024.

1. Plataforma DREX. 2. CBDC - Central Bank Digital Currency. 3. Sigilo Bancário. 4. Privacidade. 5. Criptoativos. I. Laender, Gabriel Boavista, orient. II. Título.

REFERÊNCIA BIBLIOGRÁFICA

MENDES, Fábio Luis. **Sigilo Bancário e Privacidade no DREX**. (2024). Monografia (Graduação em Direito) - Universidade de Brasília - Faculdade de Direito, Brasília, 2024. 51p.

SUMÁRIO

RESUMO	7
ABSTRACT	8
LISTA DE FIGURAS	9
LISTA DE SIGLAS E ABREVIATURAS	10
INTRODUÇÃO	11
Apresentação da pesquisa	11
Justificativa da Pesquisa	11
Problema de pesquisa	12
Estrutura da Monografia	12
Modelos Teóricos adotados	13
Papel do Estado na institucionalização dos mercados	13
Teoria da Privacidade: Integridade contextual	14
Regulação responsiva	15
Sigilo bancário e direito à privacidade	16
Direito à privacidade	16
Sigilo bancário - aspectos constitucionais	17
Sigilo bancário - aspectos legais	17
Lei Complementar nº 105, de 2001	17
Lei Geral de Proteção de Dados Pessoais (LGPD)	18
Open Finance e Open Banking	19
Sigilo bancário - doutrina e legislação	20
Sigilo bancário - dogmática do STF - jurisprudência	21
Recurso Extraordinário nº 601.314 - Tema de Repercussão Geral 225	21
HC 198643 AgR / PR - PARANÁ	23
RE 1058429 AgR / SP - SÃO PAULO	23
SPB - Sistema de Pagamentos Brasileiro	24
Introdução - arquitetura básica do sistema financeiro	24
Moeda pública e moeda privada	25
Moeda pública, soberana ou exógena	25
Moeda privada ou endógena	26
Moeda endógena e alocação privada de capital	27
Sistemas de contas de bancos centrais	28
Sistema de contas do Banco Central do Brasil	30
O sigilo bancário nas Contas de Reservas e de Liquidação	32
Sistema de Transferência de Reservas (STR)	33
Sistema de Pagamentos Instantâneos (SPI)	34

Sigilo bancário nas Contas de Pagamento Instantâneos	35
Sigilo bancário e do direito à privacidade no SPB	36
Sigilo bancário no PIX	36
Sigilo bancário no SIC - Sistema de Informações ao Cidadão	37
CBDC - moeda digital de banco central	38
CBDC - revisão bibliográfica	40
CBDC: o modelo do BIS - Bank for International Settlements	45
BIS - aspectos regulatórios e de governança	45
CBDC: modelo de dois níveis do BIS	45
CBDC: níveis de responsabilidade do banco central em relação aos dados pessoais	50
Privacidade e sigilo no modelo de duas camadas de CBDC do BIS	52
Privacidade das partes - Projeto Tourbillon do BIS	53
Anonimato do Pagador	54
CBDC - aspectos ambientais	55
DREX - CBDC do Brasil	55
Conceito - Tecnologia DLT - Registro Digital Distribuído	56
DLT baseado em conta - questões de privacidade e sigilo	57
Conceito - DEFi - Finanças Descentralizadas	59
DREX - Diretrizes de projeto	60
A arquitetura de dois níveis do DREX	61
DREX de atacado e DREX de varejo	61
DREX - DLT unificado	63
Transição para o Ledger Unificado	63
DREX - DLT do Real Digital de Atacado (wDREX) - Hyperledger Besu	64
Hyperledger Besu e Ethereum Virtual Machine (EVM)	64
Ethereum Virtual Machine - considerações sobre privacidade e sigilo	65
Anonymous Zether	66
Starlight	66
Rayls - Parchain	66
DREX - Considerações sobre privacidade	67
Teoria da privacidade - Integridade contextual no âmbito de CBDCs	67
Tensão entre a tecnologia DLT e Direito à Privacidade e ao Sigilo Bancário	68
O DLT baseado em contas do DREX - sigilo bancário e privacidade	69
Privacidade no DREX: uma questão não solucionada	71
Situação atual relativa às questões de privacidade do DREX	72
DREX - privacidade e sigilo bancário	72
A migração para o DREX aumenta a privacidade? Diminui? Mesmo nível?	73
O DREX se amolda à dogmática do STF sobre direito de privacidade e de sigilo bancário?	74
DREX - Imaginação institucional	76

O Drex é um exemplo de construção de mercado em que a privacidade é assegurada por design?	76
O Drex elimina um conjunto de instituições que asseguram o funcionamento de um mercado com mais privacidade?	77
DREX - Aspectos de Regulação responsiva	78
Conclusões	79
<u>Referências bibliográficas</u>	<u>80</u>

RESUMO

Este trabalho de conclusão de curso investiga o impacto da implementação do DREX, a versão digital do Real, sobre o direito ao sigilo bancário e à privacidade nas transações, com base em teorias sobre a institucionalização de mercados pelo Estado e na doutrina e jurisprudência do STF. Analisa como o Sistema de Pagamento Brasileiro (SPB) e a estrutura do DREX asseguram esses direitos, considerando as implicações jurídicas da migração para a moeda digital, a função dos smart contracts, e o potencial das tecnologias como Zero Knowledge (ZK) para aprimorar a privacidade. O estudo conclui identificando os desafios do DREX em relação ao direito de privacidade no âmbito da CBDC brasileira.

Palavras-chave: DREX. Sigilo Bancário. Criptomoedas. CBDC.

ABSTRACT

This dissertation explores the implications of implementing DREX, the digital version of the Brazilian Real, on the right to banking secrecy and transactional privacy within the current financial system. Grounded in theoretical frameworks about the state's role in market institutionalization and informed by constitutional doctrine and the jurisprudence of the Supreme Federal Court (STF), the research delves into how the Brazilian Payment System (SPB), managed by the Central Bank, reflects and ensures these rights. It further examines the DREX structure, its operational layers for financial institutions and citizens, and the legal challenges posed by migrating to a digital currency. This includes an analysis of DREX's architecture, the role of smart contracts, and the potential of emerging technologies like Zero Knowledge (ZK) proofs to enhance privacy and confidentiality in accordance with STF regulations. The study concludes by identifying current challenges and proposing reflections for privacy rights issues within the DREX framework.

Keywords: DREX. Banking Secrecy. Cryptocurrency. CBDC.

LISTA DE FIGURAS

Figura 1: Esquematização do STR - Sistema de Transferência de Reservas do Banco Central do Brasil

Figura 2: CBDCs - fases de implantação em 134 países

Figura 3: Arquitetura de CBDC de dois níveis do BIS - *Bank of International Settlements*

Figura 3: Níveis de privacidade e segurança das transações no modelo de CBDC do BIS

Figura 4: Modelo de CBDC Direto do BIS

Figura 5: Modelo de CBDC Hybrid do BIS

Figura 6: Modelo de CBDC Intermediated do BIS

Figura 7: Modelo de CBDC Indirect do BIS

Figura 8: Níveis de privacidade e segurança de transações de CBDC

Figura 9: Plataforma Real Digital - DREX

Figura 10: Estrutura básica do DREX

Figura 11: Transação DREX

Figura 12: Trilema de privacidade no DREX

Figura 13: Componentes do sistema Rayls

LISTA DE SIGLAS E ABREVIATURAS

BIS - *Bank of International Settlements*

CBDC - *Central Bank Digital Currency*

DREX - *Digital Real Electronic Exchange*

DLT - *Digital Ledger Technology*

EVM - *Ethereum Virtual Machine*

SPB - Sistema de Pagamentos Brasileiro

SIC - Sistema de Informações do Cidadão

SPI - Sistema de Pagamentos Instantâneos

KYC - *Know Your Client*

ZKP - *Zero Knowledge Proof*

UTXO - *Unspent Transaction Output* (saída de transação não gasta)

INTRODUÇÃO

Apresentação da pesquisa

A pesquisa tem como principal objetivo analisar se a implementação do DREX (moeda digital brasileira, Real Digital) reflete o direito ao sigilo bancário e à privacidade de transações, como presentes no sistema financeiro atual. A análise parte de modelos teóricos, como o papel do Estado na institucionalização de mercados, e explora a doutrina constitucional e a jurisprudência do Supremo Tribunal Federal (STF), que atribui natureza constitucional ao direito ao sigilo bancário. Este alicerce teórico é complementado pela introdução de uma concepção de direito de privacidade, aplicável às moedas digitais de bancos centrais (CBDC). Posteriormente, a pesquisa se aprofunda em uma análise prática, investigando como o Sistema de Pagamento Brasileiro (SPB), gerenciado pelo Banco Central, reflete e assegura o direito ao sigilo bancário e à privacidade, além de examinar como esses direitos são reproduzidos na estrutura do DREX, que considera duas camadas de operação: uma destinada às instituições financeiras e outra ao uso pelos cidadãos.

O texto então se volta para a problemática jurídica: a influência da migração para o DREX sobre a privacidade e o sigilo bancário. Essa análise inclui uma avaliação da arquitetura do DREX, considerando sua prova de conceito e a adequação ou flexibilização em relação à dogmática do STF sobre privacidade e sigilo bancário. Além disso, o estudo examina a função dos *smart contracts* no DREX e sua relação com o direito constitucional ao sigilo bancário. A seguir exploramos tecnologias potenciais, como Zero Knowledge (ZK), como forma para aprimorar o sigilo bancário e a privacidade no DREX, avaliando sua conformidade com as normativas do STF. Finalmente, a pesquisa termina na identificação dos desafios e problemas atuais do DREX em relação ao sigilo bancário e ao direito de privacidade, propondo reflexões para estas questões.

Justificativa da Pesquisa

O Banco Central do Brasil está implementando o DREX, e sua entrada em funcionamento está prevista para 2025¹. Há, porém, uma questão a ser respondida que é se a

¹ BANCO CENTRAL DO BRASIL. Nota à imprensa - Relatório de Economia Bancária de 2022. 24 ago. 2023. Disponível em: <https://www.bcb.gov.br/detalhenoticia/18170/nota>. Acesso em: 29 ago. 2024.

nova tecnologia garante os direitos constitucionais de privacidade, proteção de dados pessoais e do sigilo bancário, e em que termos, em relação ao que vige no sistema atual (Sistema de Pagamentos Brasileiro).

A experiência brasileira de desenvolvimento de uma versão digital de sua moeda não é isolada - está em um contexto mundial com bancos centrais em estágio mais ou menos avançado de implementação de suas CBDC - *Central Bank Digital Currency* - como é o caso da China, com o Yuan Digital.

Conforme o BIS², a privacidade é um requisito fundamental para as CBDCs de varejo, sendo classificadas por usuários em pesquisas realizadas pelo Banco da Inglaterra e pelo Banco Central Europeu como no topo ou próximo do topo das preocupações dos usuários.

Esse cenário sublinha a necessidade de análise das CBDCs em geral e o DREX em particular sob a ótica do direito à privacidade, buscando *insights* no modelo de CBDC do BIS - *Bank of International Settlements* - e o entendimento de como as moedas digitais em implementação estão aderentes a tais recomendações, podendo oferecer um modelo comparativo para o projeto DREX, sugerindo ajustes ou confirmando a rota escolhida pelo Banco Central do Brasil.

Problema de pesquisa

O sigilo bancário apresentado na Plataforma DREX está no mesmo nível do adotado no Sistema de Pagamentos Brasileiro?

Estrutura da Monografia

O primeiro capítulo introduz a pesquisa e relaciona os principais fundamentos teóricos usados. O segundo capítulo aborda questões doutrinárias e jurisprudenciais sobre direito de privacidade e sigilo bancário, incluindo a dogmática do STF relativamente ao sigilo bancário e ao direito de privacidade. O terceiro capítulo analisa o Sistema de Pagamentos Brasileiro, a arquitetura de contas do Banco Central, e como essa estrutura converge com o direito de privacidade e o sigilo bancário. O quarto capítulo introduz o conceito de CBDC - Central

² BANK FOR INTERNATIONAL SETTLEMENTS. Project Tourbillon: exploring a new approach to enhancing CBDC privacy and compliance. Disponível em: <https://www.bis.org/about/bisih/topics/cbdc/tourbillon.htm>. Acesso em: 29 ago. 2024.

Bank Digital Currency e descreve os modelos de CBDC propostos pelo BIS - Bank of International Settlements. O quinto capítulo descreve os principais aspectos técnicos do DREX, a CBDC brasileira, e seu sistema de contas. O sexto capítulo analisa a aderência do DREX à arquitetura constitucional, legal e jurisprudencial relativa ao sigilo bancário e ao direito de privacidade. O sétimo e último capítulo conclui a pesquisa.

Modelos Teóricos adotados

Papel do Estado na institucionalização dos mercados

Natalino Irti (IRTI, 2007) em "A ordem jurídica do mercado" apresenta uma análise crítica da percepção do mercado como fenômeno natural, rejeitando o naturalismo econômico e propondo uma visão de economia de mercado caracterizada pela artificialidade, juridicidade e historicidade. Irti argumenta contra a ideia do jusnaturalismo, que é modernamente representado na economia através da crença em leis econômicas imutáveis, as quais ele considera antijurídicas e anti-políticas.

Contrapondo-se a essa visão, Irti enfatiza que as chamadas leis “naturais” do mercado foram, de fato, historicamente definidas e moldadas por decisões humanas, fazendo do mercado um "locus artificialis". Ele salienta que o mercado demanda institutos jurídicos para funcionar corretamente e que, frequentemente, o Estado é recorrido para solucionar conflitos e descumprimentos de acordos privados. Nesse contexto, ele destaca que os acordos originários e a *lex mercatoria* (lei do comércio) não são fontes originárias do Direito, mas sim construções sociais.

Irti conclui que as decisões fundamentais que dão forma à economia e ao mercado não são resultados de forças naturais incontroláveis, mas sim atos do agir político, enfatizando o papel crucial das escolhas e intervenções humanas na configuração da ordem econômica. Ao fazer isso, ele desafia a ideia de uma economia de mercado autorregulável puramente natural, propondo uma compreensão mais complexa e realista que reconhece o papel essencial do direito e da política na formação dos mercados.

Essa perspectiva é ampliada e reforçada pelo argumento de Laender (LAENDER, 2014), em "O papel do Estado na construção da economia e a possibilidade do direito como imaginação institucional", no qual o autor sustenta que o direito não apenas molda, mas

constrói a economia, tendo uma oportunidade significativa de atuar na criação e modificação de instituições econômicas.

Alinhando isso com a introdução de um novo paradigma institucional, como a Plataforma DREX do Banco Central, percebe-se uma confluência entre os pensamentos de Irti e Laender. A Plataforma DREX representa uma inovação em termos institucionais que tem o potencial de remodelar mercados e negócios. Nesse contexto, aplicando a concepção de Irti e Laender, infere-se que o momento atual é de definição de como esses novos mercados funcionarão e como influenciarão o comportamento dos agentes, o qual será definido pela arquitetura jurídica que a Plataforma DREX adotará.

Neste contexto, o formato jurídico-institucional da Plataforma DREX não é apenas um conjunto de regras a serem seguidas, mas um mecanismo ativo de construção e reconstrução do mercado. Ela atua como um agente de imaginação institucional, onde o direito se torna uma ferramenta para inovar e criar realidades econômicas antes inexistentes.

Ademais, a Plataforma DREX tem o potencial de ser um catalisador para a transformação econômica. Ao desenhar a arquitetura jurídica da plataforma, os formuladores de políticas e reguladores têm a oportunidade de influenciar a eficiência, a segurança dos mercados, e a forma como a economia se desenvolve, inova e interage com a sociedade como um todo. Este é um exemplo prático e contemporâneo de como o direito, conforme articulado por Irti e Laender, não apenas acompanha, mas ativamente molda a economia e suas instituições.

O objeto desta Monografia é analisar uma faceta específica da arquitetura jurídica incorporada na Plataforma DREX: o direito ao sigilo bancário e a privacidade, ambos reconhecidos como direitos fundamentais constitucionalmente estabelecidos.

A análise pretende compreender a Plataforma DREX para entender como o direito ao sigilo bancário e à privacidade estão implementados nessa nova institucionalidade econômica.

Teoria da Privacidade: Integridade contextual

O desafio de conceitualizar o direito de privacidade no âmbito de moedas digitais de bancos centrais tem a contribuição de Jiang (JIANG, 2023) - que expõe a teoria da integridade

contextual, de Helen Nissenbaum, para entender a privacidade como algo determinado pelo fluxo adequado de informações pessoais dentro de normas específicas. Essa teoria considera quatro parâmetros principais: o contexto da transmissão, os atores envolvidos, os atributos da informação e o princípio que guia essa transmissão. A integridade contextual avalia a adequação do fluxo de informações baseando-se nas circunstâncias específicas e nas normas informacionais do contexto, considerando os diferentes papéis que os atores podem desempenhar (remetente, receptor, sujeito) e os atributos da informação transmitida. Essa abordagem também reconhece que a privacidade pode entrar em conflito com outros valores sociais, como na questão do tráfico de seres humanos, onde a exposição de informações privadas pode beneficiar o bem público, apresentando um desafio para a lei ao equilibrar valores conflitantes em diferentes contextos e culturas.

Jiang (2023) também explicita que o princípio de transmissão é uma norma que define o fluxo apropriado de informações entre partes em um contexto específico, baseado no motivo do remetente e na natureza da informação (voluntária, forçada, unidirecional, bidirecional, confidencial). Diferentes contextos, como saúde e amizade, podem exigir padrões distintos de confidencialidade e direção do fluxo de informação. O autor também estabelece a adequabilidade dessa concepção de direito à privacidade ao quadro jurídico das CBDCs - *Central Bank Digital Currency*.

Regulação responsiva

Ao longo desta monografia será adotada a perspectiva da Regulação Responsiva para analisar a arquitetura jurídica da Plataforma DREX, particularmente no que diz respeito à proteção do direito ao sigilo bancário e à privacidade. A Regulação Responsiva, conforme delineada por ARANHA (2023), posiciona a sanção administrativa como '*ultima ratio*' de controle, propondo um Direito Administrativo do consenso. Esta abordagem será importante para entender e avaliar a eficácia da regulação do Banco Central e sua interação com os múltiplos operadores privados na Plataforma DREX, que inclui bancos comerciais, instituições de pagamento, e também empresas de tecnologia que fornecem as soluções para o DREX.

No âmbito da Plataforma DREX, o Banco Central, enquanto órgão regulador, pode adotar princípios de regulação responsiva para promover um ambiente que proteja os direitos de privacidade e sigilo bancário, e incentive a inovação.

Ao adotar a lente da Regulação Responsiva, esta Monografia buscará compreender como a regulação da Plataforma DREX está sendo estruturada para proteger direitos fundamentais, promover a inovação e facilitar a colaboração entre os diversos *stakeholders*.

Sigilo bancário e direito à privacidade

Direito à privacidade

O direito à privacidade é tratado doutrinariamente (BLUM, 2022) abrangendo a intimidade e a vida privada, previstos no art. 5º, X, da CF88: “são invioláveis a **intimidade**, a **vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”.

Conforme BLUM (2022), José Afonso da Silva e outros estudiosos, como Renan Lotufo e Paulo José da Costa Jr., fazem uma distinção entre os conceitos de "intimidade" e "vida privada" no contexto da proteção constitucional brasileira. A "intimidade" refere-se a um círculo muito restrito de informações e interações pessoais, que um indivíduo escolhe compartilhar apenas com pessoas de sua máxima confiança. Em contrapartida, a "vida privada" abrange um espectro mais amplo, incluindo dados e comportamentos que o indivíduo prefere não se tornem públicos, mas que podem ser conhecidos por um círculo maior de pessoas. Costa Jr. utiliza o conceito de círculos concêntricos para ilustrar essa diferença, onde a intimidade é um círculo mais interno e restrito dentro da esfera maior da privacidade.

Essa diferenciação é fundamental para entender a amplitude e a aplicação das proteções legais. A Constituição Brasileira assegura a inviolabilidade tanto da intimidade quanto da vida privada, garantindo compensações por danos quando há violação desses direitos. A proteção à vida privada e à intimidade é especialmente pertinente na era digital, onde o controle sobre os próprios dados e informações pessoais é constantemente desafiado. A teoria dos círculos de Costa Jr. destaca a necessidade de uma proteção jurídica mais intensa conforme se penetra nos círculos mais íntimos e confidenciais da vida de uma pessoa.

Sigilo bancário - aspectos constitucionais

A índole constitucional do sigilo bancário é abordada por Mendes e Martins (1992, p. 435) ao analisarem os requisitos para a quebra de sigilo bancário por Comissões Parlamentares de Inquérito (CPI) - os quais devem estar alinhados com as disposições da Lei nº 4.595 de 1964. Contudo, os autores também argumentam que esses requisitos devem ser interpretados e aplicados em consonância com as premissas normativas estabelecidas no artigo 93, inciso IX, da Constituição Federal de 1988.

Essa interpretação concede ao sigilo bancário uma natureza constitucional, garantindo que a sua quebra ocorra de maneira justificada e em situações excepcionais, assegurando, assim, a proteção dos direitos fundamentais dos cidadãos. Mendes e Martins (1992) ressaltam, ainda, a importância de equilibrar a necessidade de investigação pelas comissões parlamentares de inquérito com a proteção à privacidade financeira dos indivíduos, de acordo com os princípios constitucionais.

De Sousa (2020) sustenta que o sigilo bancário, apesar de protegido como um direito fundamental pela Constituição Federal de 1988, não é absoluto e pode ser relativizado em determinadas situações. Conforme a Lei Complementar 105, de 2001, o Banco Central, a Comissão de Valores Mobiliários e as instituições financeiras devem fornecer informações sigilosas ao Poder Legislativo Federal para fins de fiscalização, respeitando o processo legal e a aprovação do Plenário ou das comissões parlamentares de inquérito. Adicionalmente, a mesma lei permite que agentes fiscais acessem documentos financeiros durante procedimentos fiscais. A jurisprudência e doutrina enfatizam a necessidade de intervenção judicial e respeito ao devido processo legal, garantindo que a quebra do sigilo se justifique por um interesse público preponderante e seja proporcional, alinhando-se aos princípios de privacidade e intimidade estabelecidos na Constituição.

Sigilo bancário - aspectos legais

Lei Complementar nº 105, de 2001

O art. 1º da Lei Complementar nº 105, de 10 de janeiro de 2001, estabelece que: “as instituições financeiras conservarão sigilo [grifos nossos] em suas operações ativas e passivas e serviços prestados”.

A própria Lei Complementar nº 105, de 2001, estabelece as flexibilizações no sigilo das operações, equilibrando a necessidade de confidencialidade com a transparência e a segurança nas operações financeiras. Esta flexibilização não é considerada uma violação do dever de sigilo, desde que respeite certas condições e finalidades específicas:

- troca de informações entre instituições financeiras para fins cadastrais, inclusive através de centrais de risco;
- compartilhamento de dados de emitentes de cheques sem fundos e de devedores inadimplentes com entidades de proteção ao crédito;
- fornecimento de informações sobre operações financeiras em casos específicos, como em situações que envolvam suspeitas de ilícitos penais ou administrativos, incluindo operações com recursos provenientes de práticas criminosas;
- fornecimento de dados financeiros a gestores de bancos de dados para a formação de histórico de crédito.

Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei nº 13.709, de 14 de agosto de 2018³ - Lei Geral de Proteção de Dados Pessoais (LGPD), institui diretrizes para tratamento de dados pessoais por pessoas físicas, instituições públicas e empresas privadas, buscando resguardar o direito fundamental de privacidade.

Essa legislação define, em seu art. 5º, o que é “dado pessoal” - informações de pessoas físicas identificadas ou que possam ser identificadas de alguma maneira e de que forma podem ser tratadas, e o conceito de “controlador de dados” - pessoa física ou jurídica responsável pelas decisões sobre tratamento de dados pessoais. No caso do Sistema Financeiro Nacional, o controlador de dados pessoais é o Banco Central do Brasil. Já o art. 7º da LGPD estabelece normas para operações com dados pessoais por pessoas físicas ou por empresas, órgãos e entidades públicos.

³ BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei n.º 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 29 ago. 2024.

Open Finance e Open Banking

A proteção de dados pessoais no âmbito do Sistema Financeiro Nacional tem um tratamento específico por meio da Resolução BCB nº 32, de 29 de outubro de 2020 - o qual estabelece os requisitos técnicos e procedimentos operacionais para a implementação de um Sistema Financeiro Aberto no Brasil, definindo requisitos e normas para ampliação de competição no Sistema Financeiro Brasileiro, regulamentando o compartilhamento de dados pessoais e aplicações entre instituições que participam do Sistema Financeiro Nacional.

Em 2019 iniciou-se os testes para a implementação do conceito de Open Banking no Brasil - uma iniciativa que permite compartilhamento de dados, produtos e serviços entre instituições financeiras com o objetivo de, por meio de aumento de eficiência e a competição, oferecer serviços financeiros de maior qualidade aos cidadãos. A implementação do sistema ocorreu a partir de 2020.

Posteriormente, o Banco Central do Brasil ampliou o conceito de Open Banking para o de Open Finance⁴, também objetivando a implantação de um sistema financeiro aberto, mas agora com possibilidade dos clientes de produtos e serviços financeiros compartilhar informações entre diferentes instituições autorizadas pelo Banco Central, de modo a permitir o compartilhamento de informações bancárias entre diferentes plataformas, para além dos sistemas da instituição financeira a qual a pessoa está vinculada.

Por meio dessa sistemática, há a possibilidade de instituições financeiras se conectarem aos sistemas de outras para acesso às informações financeiras de clientes, mediante sua permissão e consentimento. A regulação desses processos é feito atualmente pela Resolução BCB nº 32, de 29 de outubro de 2020, com redação dada pela Resolução BCB nº 398, de 4 de julho de 2024⁵.

Essa legislação estabelece os requisitos técnicos e os procedimentos operacionais para a implementação no Brasil do Open Finance, definindo o escopo de abrangência da norma:

⁴ BANCO CENTRAL DO BRASIL. **Open Finance**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/openfinance>. Acesso em: 29 ago. 2024.

⁵ BANCO CENTRAL DO BRASIL. **Resolução BCB nº 32, de 29 de outubro de 2020**. Dispõe sobre a implementação de política de continuidade de negócios para o mercado financeiro. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=32>. Acesso em: 29 ago. 2024.

instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

Ademais, detalha os requisitos técnicos e operacionais - abordados em manuais técnicos emitidos pelo Banco Central - e especifica os dados e serviços que devem ser compartilhados pelas instituições participantes, abrangendo informações sobre canais de atendimento, produtos e serviços, bem como tarifas e taxas de juros.

Há ainda definições de natureza técnica de tecnologia da informação para padronizar o desenvolvimento e uso de aplicações financeiras com a finalidade de permitir a interoperabilidade dos dados.

É importante apontar que na instituição do Open Finance o Banco Central adota uma abordagem regulatória responsiva. Nos termos propostos por Aranha (ARANHA, 2023), pode-se observar que o Banco Central do Brasil estabeleceu uma estrutura de governança que busca a promoção de um consenso e o estabelecimento de um diálogo construtivo entre reguladores e regulados.

O Banco Central criou uma Estrutura de Governança⁶, que reúne os participantes, fomentando o diálogo para implementação do ecossistema de um Sistema Financeiro Aberto, sendo que a autoridade monetária acompanha todas as discussões de forma a assegurar que as diretrizes regulatórias sejam observadas.

Sigilo bancário - doutrina e legislação

Conforme Abraão (2019), o sistema legal brasileiro em relação ao sigilo bancário compartilha semelhanças com o modelo adotado na Europa continental, que aborda a matéria como um segredo profissional. No Brasil, tanto o Código de Processo Civil (art. 448, II) quanto ao Código de Processo Penal (art. 207) - ambos proíbem a revelação de informações obtidas por profissionais em razão de suas funções. Além disso, o art. 154 do Código Penal brasileiro criminaliza a divulgação dessas informações sem justa causa.

⁶OPEN FINANCE BRASIL. **Open Finance Brasil**. Disponível em: <https://openfinancebrasil.org.br/>. Acesso em: 29 ago. 2024.

Especificamente sobre o sigilo bancário, retomamos a Lei Complementar nº 105, de 2001, a qual desempenha um papel fundamental. Essa Lei, como mostramos acima, estabelece as condições sob as quais o sigilo bancário pode ser quebrado, priorizando o interesse público sobre a privacidade dos clientes - convergindo com a concepção contextual do direito à privacidade exposto por Jiang (2023). As situações que permitem a quebra do sigilo são limitadas e bem definidas (*numerus clausus*), principalmente visando combater o crime organizado, lavagem de dinheiro, tráfico de drogas, e delitos contra a ordem tributária e a previdência social.

Ainda segundo Abrão (2019), a legislação atual sobre o sigilo bancário não é inflexível em termos de princípios. Em vez disso, ela enfatiza a importância do papel do Estado no combate ao crime organizado e outros delitos graves, permitindo a quebra do sigilo em casos específicos e sob a iniciativa da Administração Pública. Esse equilíbrio reflete a necessidade de proteger tanto a privacidade individual quanto o interesse público, especialmente no contexto de crimes financeiros e fiscais complexos.

Sigilo bancário - dogmática do STF - jurisprudência

Após relacionarmos as principais disposições de natureza doutrinária, constitucional e legal sobre o direito ao sigilo bancário, passamos a explorar como o tema vem sendo tratado pelo STF - Supremo Tribunal Federal - em suas decisões.

Recurso Extraordinário nº 601.314 - Tema de Repercussão Geral 225⁷

O julgamento do RE nº 601.318 discutiu a constitucionalidade do art. 6º da Lei Complementar nº 105/2001, que permitiu o fornecimento de informações sobre movimentações financeiras diretamente ao Fisco, sem autorização judicial, e fixou a tese do Tema 225 segundo a qual “o art. 6º da Lei Complementar nº 105/01 não ofende o direito ao sigilo bancário, pois realiza a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva, bem como estabelece requisitos objetivos e o traslado do dever de sigilo da esfera bancária para a fiscal”.

⁷ BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário n.º 601.314/RS**. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=2689108&numeroProcesso=601314&classeProcesso=RE&numeroTema=225>. Acesso em: 29 ago. 2024.

O acórdão traz à tona o debate sobre a interação entre direitos individuais e obrigações fiscais, destacando o equilíbrio necessário entre o direito ao sigilo bancário e o dever de pagar tributos. As citações extraídas do texto do acórdão revelam uma análise por parte dos Ministros sobre como esses dois aspectos se relacionam dentro de uma estrutura constitucional, refletindo sobre a finalidade da tributação e seu impacto na sociedade e no indivíduo.

O texto aponta que *“em um confronto entre o direito ao sigilo bancário e o dever de pagar tributos, ambos referidos a um mesmo cidadão e de caráter constituinte no que se refere à comunidade política, à luz da finalidade precípua da tributação de realizar a igualdade em seu duplo compromisso, a autonomia individual e o autogoverno coletivo”* e destaca que tanto o sigilo bancário quanto o dever de pagar tributos são componentes essenciais que coexistem dentro da mesma esfera de direitos e deveres de um cidadão, moldados pela Constituição. Essa interação é vista como uma forma de promover a igualdade, respeitando tanto a autonomia individual quanto o autogoverno coletivo.

Prossegue para descrever a importância do sigilo bancário na proteção da autonomia individual, afirmando que *“Do ponto de vista da autonomia individual, o sigilo bancário é uma das expressões do direito de personalidade que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira.”* Esta passagem reforça o sigilo bancário como um direito fundamental que protege as informações pessoais contra intervenções não autorizadas.

Na perspectiva do autogoverno coletivo, o texto ressalta que *“a igualdade é satisfeita no plano do autogoverno coletivo por meio do pagamento de tributos, na medida da capacidade contributiva do contribuinte, por sua vez vinculado a um Estado soberano comprometido com a satisfação das necessidades coletivas de seu Povo.”* Isso sublinha a importância dos tributos para a sustentabilidade e o bem-estar coletivo, garantindo que cada indivíduo contribua de acordo com sua capacidade econômica.

Por fim, o acórdão aborda a regulamentação dessa relação, especificando que *“o Poder Legislativo não desbordou dos parâmetros constitucionais, ao exercer sua relativa liberdade de conformação da ordem jurídica, na medida em que estabeleceu requisitos*

objetivos para a requisição de informação pela Administração Tributária às instituições financeiras, assim como manteve o sigilo dos dados a respeito das transações financeiras do contribuinte, observando-se um traslado do dever de sigilo da esfera bancária para a fiscal.” Essa parte conclui que o art. 6º é constitucionalmente válido, e, portanto, as autoridades tributárias podem examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, no curso de processos administrativos ou de procedimento fiscal, não sendo necessária decisão judicial.

HC 198643 AgR / PR - PARANÁ⁸

No julgamento do Agravo Regimental no *Habeas Corpus* nº 198.643, o STF discutiu a extensão da garantia constitucional do sigilo bancário, apontando que a jurisprudência reconhece que a intimidade e a privacidade das pessoas tem, como um de seus corolários, a proteção ao sigilo de dados bancários e fiscais.

Porém, tais direitos não são absolutos, podendo ser quebrados presentes os requisitos: demonstração de indícios de existência de delito; demonstração da necessidade/imprescindibilidade da medida para obtenção de prova da autoria e/ou materialidade do delito; indicação da pertinência temática entre as informações obtidas e a natureza do delito; delimitação dos sujeitos titulares dos dados a serem investigados e do lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira.

No caso concreto analisado pelo STF, considerou-se constitucional o entendimento das instâncias ordinárias sobre a possibilidade de quebra de sigilo bancário embasada em declarações realizadas no âmbito de colaboração premiada.

RE 1058429 AgR / SP - SÃO PAULO⁹

A análise e deliberação deste Recurso Extraordinário, os Ministros do STF assentaram o entendimento segundo o qual o Ministério Público pode solicitar diretamente ao COAF

⁸ BRASIL. Supremo Tribunal Federal. **Jurisprudência do STF**. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur444467/false>. Acesso em: 29 ago. 2024.

⁹ BRASIL. Supremo Tribunal Federal. **Jurisprudência do STF**. Disponível em: <https://jurisprudencia.stf.jus.br/pages/search/sjur381351/false>. Acesso em: 29 ago. 2024.

(atualmente UIF¹⁰) dados financeiros. “Se a legislação de regência impositivamente determina que o COAF “comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito” (art. 15 da Lei 9.613/1998), seria contraditório impedir o Ministério Público de solicitar ao COAF informações por esses mesmos motivos.”

Conforme LUZ (2019), o Brasil aderiu ao Programa “*Foreign Account Tax Compliance Act – FACTA*”, o qual permite aos EUA enviar ao Governo brasileiro informações que se referem às contas correntes e situações patrimoniais de brasileiros disponíveis no sistema financeiro americano, e conclui que a jurisprudência tanto do STF quanto do STJ garantem o sigilo das informações financeiras (bancário ou fiscal), relativizando, porém, em atendimento ao primado do interesse público frente ao particular, que a Administração Tributária tem acesso às informações financeiras mediante processo administrativo ou fiscalização em curso, “hipóteses em que não mais será oponível o sigilo”.

Já no âmbito do setor privado, as entidades que lidam com informações financeiras e fiscais devem manter sob sigilo tais informações.

SPB - Sistema de Pagamentos Brasileiro

Introdução - arquitetura básica do sistema financeiro

Salama e Zelmanovitz (2023) elucidam a estrutura dos sistemas financeiros atuais que operam sob um sistema monetário dual, com dois níveis: o nível superior, ocupado pelo banco central, e o nível inferior, composto pelos bancos comerciais. Os usuários desse sistema têm duas principais formas de realizar pagamentos: utilizando moeda física estatal, que é produzida pelo banco central, ou através de depósitos em conta corrente, que são criados pelos bancos comerciais, definidos pelos autores como moeda privada.

Nesse contexto, os autores notam que os depósitos em conta corrente, tecnicamente, não são considerados moeda. No entanto, devido à sua ampla aceitação e capacidade de

¹⁰ BRASIL. Ministério da Fazenda. **Inteligência Financeira**. Disponível em: <https://www.gov.br/fazenda/pt-br/assuntos/prevencao-lavagem-dinheiro/inteligencia-financeira>. Acesso em: 29 ago. 2024.

facilitar transações financeiras de maneira eficiente, eles possuem muitas características atribuídas às moedas.

Moeda pública e moeda privada

Salama e Zelmanovitz (2023) sustentam que o que se conhece como finanças modernas, a feição institucional atual dos sistemas financeiros nacionais, foi criada no final do século XVII, precisamente em 1694 com a criação do *Bank of England* (Salama, Zelmanovitz, 2003, p5). E é caracterizado pelo fato de a moeda de uso comum ser criada parcialmente pelo Estado, e parcialmente pelo mercado.

Moeda pública, soberana ou exógena

Sendo assim, conforme Salama e Zelmanovitz (2023), circulam predominantemente na economia dois tipos de moedas, as moedas estatais (soberanas), que são emitidas pelo Estado, e representam uma obrigação do titular contra o Banco Central, estas são as “moedas públicas”, também apontadas pelos autores como moeda “exógena”, no sentido que sua criação não ocorre em função demandas de moeda geradas no próprio mercado, mas por uma determinação política. Nos termos dos autores (Salama, Zelmanovitz, 2003, p5):

“É comum traçar uma divisão rígida entre a moeda commodity (especialmente metálica) e a moeda fiat, e é natural que seja assim. Mas há entre elas uma semelhança importante: ambas são fornecidas pelo governo e são determinadas, portanto, “fora” do mercado. Não são moedas endógenas, geradas a partir da demanda por moeda, mas moedas exógenas, no sentido de serem criadas para atender diretamente a um comando político. É por isso, que esta moeda exógena é também chamada de “soberana”, “estatal” ou “pública”.

Nesse contexto, são moedas públicas, ou moedas soberanas, o papel moeda (dinheiro em espécie) nas mãos da população, e os depósitos dos bancos comerciais nas chamadas contas de reserva, que são as contas mantidas pelas instituições financeiras no Banco Central.

Essas duas formas monetárias são tecnicamente consideradas moedas por representarem um direito do titular (o detentor do papel moeda em espécie ou o titular da

conta de reserva no Banco Central) perante o Banco Central. Ou dito de outra forma, uma obrigação do Banco Central perante os titulares.

É importante apontar, porém, que na atualidade, o papel moeda em circulação na economia se reduziu drasticamente, de modo que a maior parte da moeda “soberana” efetivamente está nas contas de reservas do Banco Central mantidas pelas instituições financeiras.

Como veremos a seguir, transportando esses conceitos para as CBDC, o formato digital das moedas nacionais, a moeda pública, soberana ou exógena será representada no sistema DREX pelo “DREX de atacado”, ou seja, o wDREX.

Moeda privada ou endógena

O segundo tipo de moeda que circula nas economias modernas é definido por Salama e Zelmanovitz (2023) como moeda privada, ou moeda endógena. Segundo os autores, as moedas privadas são criadas pelos bancos comerciais, mediante depósitos à vista nas contas mantidas pelos clientes nos bancos comerciais.

Os autores (Salama e Zelmanovitz, 2023, p6), apontam que *é “claro que, no que toca à sua circulação e uso como meio de pagamento, a moeda privada bancária acaba por corresponder em quase todas as situações à moeda pública”* (grifos nossos). O Código Civil Brasileiro, em seu art. 315, estabelece que *“dívidas em dinheiro deverão ser pagas no vencimento, em moeda corrente”*, mas as transferências de saldos entre contas de bancos comerciais (moeda escritural ou moeda bancária) são convencionalmente equiparadas à moeda.

Essas características, somada à grande aceitação das transferências de saldos de depósitos à vista como meio de pagamento, e, ainda o fato de o Tesouro Nacional aceitar tais transferências como pagamento de tributos *“confere a esta moeda privada na prática um status muito similar àquele dado à moeda estatal”* (Salama e Zelmanovitz, 2023, p6).

Entretanto, há uma diferença fundamental entre estas moedas privadas, os depósitos à vista, e a moeda soberana, que é o fato de elas representarem um direito do titular perante o banco comercial, e não um direito do titular perante o Banco Central. Os autores apontam,

ainda, que esta moeda privada é “endógena” porque sua emissão decorre de uma demanda no mercado, que se materializa na forma de demanda por crédito para a implementação de projetos de investimento. Diferentemente da moeda soberana, ou exógena, que é emitida por determinação política.

Mais adiante veremos que, na transposição desses conceitos para o formato digital das moedas nacionais, CBDC, no caso brasileiro, o DREX, essa moeda privada, os depósitos à vista, são representados pelo DREX de varejo, *r*DREX, emitido pelos bancos comerciais, na forma de uma *stable coin* privada, com paridade de valor com a moeda nacional soberana.

Moeda endógena e alocação privada de capital

Apesar de não poderem ser considerados tecnicamente como “moedas”, os depósitos bancários são tratados por Salama e Zelmanovitz (2023) como moedas privadas. Os autores apontam a complexidade dos sistemas monetários modernos, nos quais os bancos comerciais desempenham um papel fundamental na criação de "moedas privadas" por meio da concessão de empréstimos mediante avaliação de projetos de investimento. Essa prática permite aos bancos comerciais “criar moeda”, sendo esse processo parte da implementação de alocação privada de capital, dentro de um sistema regulado que, tradicionalmente, reserva ao banco central o monopólio da emissão de moeda, conforme estabelecido pelo artigo 164 da Constituição Federal de 1988 - “*art. 164. A competência da União para emitir moeda será exercida exclusivamente pelo **banco central***”.

No entanto, o mesmo artigo, por meio de seu §1º, também restringe o banco central de conceder empréstimos diretamente a entidades que não sejam instituições financeiras, limitando assim sua atuação na alocação direta de capital. Isso delega aos bancos comerciais a responsabilidade primária de financiar cidadãos e empresas, criando uma moeda "endógena", que se ajusta automaticamente à oferta e demanda por meio das operações bancárias. Em contraste, a moeda emitida pelo banco central é considerada "exógena" por sua natureza política e externa às forças de mercado.

Os bancos comerciais, porém, são limitados na criação dessa moeda endógena (depósitos bancários) devido ao sistema de reservas fracionárias. Esse sistema exige que os bancos mantenham uma reserva no banco central, uma fração dos depósitos à vista nas contas

dos clientes, sendo essa reserva uma garantia para as emissões de moeda. Esse mecanismo reduz o risco de corridas bancárias e mantém a estabilidade financeira.

Posteriormente, o sistema financeiro inclui um novo tipo de ator apto a atuar no sistema de atacado do sistema financeiro - as "instituições de pagamento", definidas na Lei nº 12.865 de 2013¹¹, e que podem emitir moeda eletrônica, mas totalmente lastreada em moeda física ou escritural, impedindo-as, portanto, de criar moeda da maneira como os bancos comerciais o fazem.

Mais adiante estudaremos a arquitetura das moedas digitais (CBDC), mas antecipamos que um *design* de CBDC (*Central Bank Digital Currency*) de apenas um nível, ou seja, operada diretamente pelo Banco Central, desafiaria esses fundamentos, ao possibilitar que os usuários finais tivessem contas diretamente no Banco Central, potencialmente reduzindo o papel dos bancos comerciais na alocação de capital e aumentando o controle estatal sobre as transações e a economia. Apesar de, do ponto de vista tecnológico ser possível, há muitos inconvenientes nessa solução, como aponta Jiang (2023), entre os quais seria um desvio de finalidade do Banco Central - cuja responsabilidade é de executar e controlar a política monetária do País, e não de cuidar de contas e pagamentos de clientes.

Diante desse contexto, e também para se adequar à moldura constitucional e institucional vigente, o modelo de CBDC que está fase de desenvolvimento no Brasil, o DREX é uma CBDC de dois níveis operacionais, formada por uma CBDC de atacado, conforme o planejamento do DREX de atacado, focada no uso interbancário, alinhando-se com os requisitos constitucionais, buscando manter os papéis dos atores do sistema financeiro atual. Há ainda um DREX de varejo, que será emitido e controlado pelos bancos comerciais - sendo uma versão digital dos depósitos bancários.

Sistemas de contas de bancos centrais

Após a introdução sobre o funcionamento básico do sistema financeiro, das moedas soberanas e das moedas privadas, vamos aprofundar a distinção das funções entre banco central e bancos comerciais. Mehrling (2011) aponta que os bancos comerciais são as

¹¹ BRASIL. **Lei n.º 12.865, de 9 de outubro de 2013**. Dispõe sobre os arranjos de pagamento e as instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB). Diário Oficial da União: seção 1, Brasília, DF, 10 out. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/ato2011-2014/2013/lei/112865.htm. Acesso em: 29 ago. 2024.

instituições primordiais na economia capitalista, visto que são os bancos comerciais que administram o sistema de pagamentos de varejo. A maior parte das transações - compras e vendas de bens e serviços - é realizada por meio de transferências de depósitos à vista entre compradores e vendedores.

Os bancos centrais têm uma função diferente dentro do sistema. Os bancos centrais não operam o sistema de pagamentos de varejo. Entretanto, conforme Mehrling (2011), o banco central é considerado o banco dos bancos, ou o banco supremo, porque ele administra e controla o sistema de pagamentos no atacado, utilizado pelos próprios bancos comerciais para operarem transferências de disponibilidades financeiras entre si, por meio das chamadas contas de reserva, mantidas no banco central por cada um dos participantes do sistema financeiro.

Diariamente, famílias, empresas, governos transacionam bens e serviços e essas transações são executadas por meio do sistema de pagamentos de varejo administrado pelos bancos comerciais. Mas há múltiplos bancos comerciais em operação, assim como as instituições de pagamento, e cada banco ou instituição de pagamento gerencia seu fluxo de entradas e saídas diárias de moeda. Os clientes recebem e enviam recursos para outras instituições financeiras, de modo que ao final do dia cada banco verifica o total de recursos recebidos e os enviados por seus clientes para outros bancos, e enviam e recebem recursos para os outros participantes do sistema financeiro por meio das contas de reserva que mantém no Banco Central.

Dessa forma, quando um banco realiza um pagamento a outro, ocorre uma alteração nos registros do balanço do banco central, refletindo um débito na conta do banco pagador e um crédito na conta do banco receptor. Os bancos não podem ficar com saldos negativos nas contas de reservas, e devem liquidar todos os pagamentos realizados pelos clientes durante o dia. Caso um banco fique temporariamente sem recursos, o Banco Central atua como “emprestador de última instância”, fornecendo moeda para que esse banco liquide todos os pagamentos com outros bancos e participantes. Essa exigência de liquidar pagamentos diariamente nos registros do banco central constitui uma disciplina importante para manter a integridade do sistema.

Como vimos anteriormente, e conforme Salama e Zelmanovitz (2023), além de administrar o sistema de pagamentos de varejo, os bancos comerciais também criam moeda privada, por meio de criação de depósitos à vista (moeda privada) mediante análise de propostas de investimentos potencialmente lucrativos. Nesse sentido, os bancos comerciais que fazem a alocação privada de capital por meio de alocação de empréstimos.

Entretanto, conforme Mehrling (2011), a estrutura institucional e regulatória do sistema de financiamento permite que o banco central - apesar de não operar diretamente o sistema de crédito - controle as operações de crédito, impedindo que ocorram transações fora do escopo definido pelas autoridades reguladoras - o próprio Banco Central, CVM - Comissão de Valores Mobiliários, Tesouro Nacional, Ministério da Fazenda, entre outros. Essa arquitetura tem o objetivo de tornar impraticável alocar crédito de maneira preferencial para fins não socialmente benéficos.

O autor ainda relaciona que todas as pessoas estão sujeitas a restrições financeiras, e para os bancos essa restrição se manifesta especificamente como uma 'restrição de reservas' (sistemas de reservas fracionárias) uma vez que os bancos devem liquidar os saldos devedores de suas contas de reservas diariamente.

Atualmente, e desde 2002 (Santana, 2005, p66), as contas de Reservas Bancárias do Sistema de Pagamentos Brasileiro são monitoradas pelo Banco Central em tempo real, e não são permitidos saldos negativos em qualquer momento do dia. Eventuais saldos negativos devem ser cobertos ou por meio de recursos próprios da instituição de pagamento, ou por intermédio de empréstimos intradia oferecidos pelo BCB aos bancos, operações estas denominadas “redesconto”.

Sistema de contas do Banco Central do Brasil

As instituições participantes do Sistema Financeiro Nacional e do Sistema de Pagamentos Brasileiro mantêm contas no Banco Central do Brasil: Conta de Reservas Bancárias; Contas de Liquidação; e Conta Única do Tesouro Nacional, conforme Resolução BCB nº 105 de 9 de junho de 2021¹².

¹² Resolução BCB 105/2021 BANCO CENTRAL DO BRASIL. **Resolução BCB nº 105, de 9 de junho de 2021.** Estabelece critérios e procedimentos para avaliação de produtos e serviços financeiros. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=105>. Acesso em: 29 ago. 2024.

A **Conta de Reservas Bancárias** tem como finalidade manter disponibilidades de instituições financeiras bancárias em moeda nacional no Banco Central do Brasil (Bacen). Ela permite que estas instituições mantenham seus saldos de liquidez no Bacen, permitindo o cumprimento de suas obrigações e a execução de operações de pagamento.

A Conta de Liquidação, por sua vez, é de titularidade das câmaras e dos prestadores de serviços de compensação e de liquidação, dos fundos garantidores de crédito e das demais instituições autorizadas a funcionar pelo Banco Central do Brasil que não possam ser titulares de conta Reservas Bancárias, e são mantidas no Banco Central do Brasil para fins de acolhimento dos depósitos dessas instituições e de transferência de fundos no âmbito do STR.

Estrutura das Contas e Tipos de Participantes		
Manutenção	Conta Reservas Bancárias	Conta de Liquidação
Obrigatória	<ul style="list-style-type: none"> •Banco Comercial •Banco Múltiplo com carteira comercial •Caixa Econômica 	Câmara/prestador de serviços de compensação e de liquidação sistemicamente importante (B3, SELIC)
Facultativa	<ul style="list-style-type: none"> •Banco de Desenvolvimento •Banco de Investimento •Banco de Câmbio •Banco Múltiplo sem carteira comercial 	Câmara/prestador de serviços de compensação e de liquidação não sistemicamente importante
		<ul style="list-style-type: none"> • Instituição de Pagamento • Demais Instituições autorizadas a funcionar pelo BCB (corretoras e distribuidoras de valores mobiliários, consórcios, cooperativas de crédito e sociedades de arrendamento mercantil)

Tabela: Estrutura de contas por tipo de participante - fonte BCB¹³

No Sistema de Pagamentos Brasileiros, uma instituição bancária não pode manter conta em outra instituição bancária¹⁴, de modo que todos os pagamentos têm liquidação final ou na conta Reservas Bancárias ou na Conta de Liquidação, exceto os realizados em papel moeda (espécie).

As Contas de Reservas Bancárias e as Contas de Liquidação apresentam aspectos similares, como o fato de que devem sempre apresentar saldo maior ou igual a zero, nos termos do art. 8º da Circular nº 3.438 do BACEN, de modo que a transferência de fundos originada nas contas de reservas ou de liquidação promove a alteração nos saldos das contas envolvidas, para todos os fins, exclusivamente no momento em que realizada.

A Conta de Liquidação é usada também para liquidar obrigações financeiras entre as instituições titulares da conta e o Banco Central do Brasil (Bacen) e para movimentações dentro do STR.

O sigilo bancário nas Contas de Reservas e de Liquidação

Note-se que na sistemática vigente do SPB, as instituições que mantêm contas (Reservas Bancárias ou Contas de Liquidação) diretamente junto à autoridade monetária, como bancos comerciais, instituições de pagamentos, entre outras, têm assegurado o sigilo dessas contas mediante um arcabouço legal e infralegal.

No nível legal, o dever de o Banco Central de conservar o sigilo bancário de suas operações está insculpido na Lei Complementar nº 105, de 2001, conforme a inteligência do art. 1º, §1º, I: “*Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados. §1º São consideradas instituições financeiras, para os efeitos desta Lei Complementar: I – os **bancos de qualquer espécie.***”

Esse entendimento é convergente com Steinberg e Espir (Steinberg, Espir, 2023) que enfatizam que pelas regras da Lei Complementar nº 105, de 2001, o Banco Central deve

¹³ BANCO CENTRAL DO BRASIL. **Tutorial Internet STR**. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/estabilidade_docs/Tutorial_Internet_STR.pdf. Acesso em: 29 ago. 2024.

¹⁴ BANCO CENTRAL DO BRASIL. **Circular n.º 3.438, de 2 de março de 2009**. Disponível em: https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/47671/Circ_3438_v1_O.pdf. Acesso em: 29 ago. 2024.

respeitar as regras de sigilo, de modo que todas as operações realizadas nessas contas são de conhecimento do Banco Central e dos titulares das contas, apenas.

A conta Reservas Bancárias e a Conta de Liquidação têm a regulamentação infralegal estabelecida na Resolução BCB nº 105, de 2021, que determina, por intermédio do seu art. 5º, IV, que o Bacen “*observa as disposições legais aplicáveis ao sigilo de **dados***”. A mesma norma estabelece no art. 26 - que trata dos direitos do participante do STR - inciso II, alínea “c)” que há o “*direito de conhecer tempestivamente o saldo de sua conta ao final do período de funcionamento de cada dia*”. O art. 27, que trata dos deveres dos participantes do STR, define no inciso II que devem “*zelar pela segurança e pelo sigilo das ordens de transferência de fundos por ele emitidas e recebidas e pelo bom funcionamento do STR*”.

Toda essa arquitetura jurídica implementa o sigilo bancário e a privacidade de dados pessoais no âmbito do Sistema de Transferência de Reservas do Banco Central - que, como exploramos a seguir, é mercado financeiro de atacado ou “interbancário”.

Sistema de Transferência de Reservas (STR)

O Sistema de Transferência de Reservas (STR) é o coração do Sistema de Pagamentos Brasileiro (SPB), no qual ocorre a liquidação de todas as obrigações financeiras no Brasil, instituições bancárias, instituições de pagamentos¹⁵, câmaras de compensação e liquidação, e fundos garantidores de crédito.

Nesse contexto, qualquer transferência de fundos entre entidades autorizadas a operar dentro do STR sempre deve ocorrer via STR, o qual é mantido e gerenciado pelo Banco Central do Brasil.

Para participar do STR, as instituições financeiras e de pagamentos devem ter contas próprias no Banco Central (as referidas Contas de Reservas Bancárias ou Contas de Liquidação). As instituições acessam o STR para emitir e receber ordens de transferência, gerenciar saldos de contas e realizar outras operações.

¹⁵ Instituição de pagamento (IP) é a pessoa jurídica que viabiliza serviços de compra e venda e de movimentação de recursos, no âmbito de um arranjo de pagamento, sem a possibilidade de conceder empréstimos e financiamentos. BANCO CENTRAL DO BRASIL. **Instituição de Pagamento**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/instituicaoopagamento>. Acesso em: 29 ago. 2024.

Os participantes devem manter saldo igual ou superior a zero nas contas para assegurar a execução das transferências. A insuficiência de saldo leva a ordem de transferência à lista de espera do STR, processada apenas com o cancelamento da ordem ou ingresso de recursos na conta.

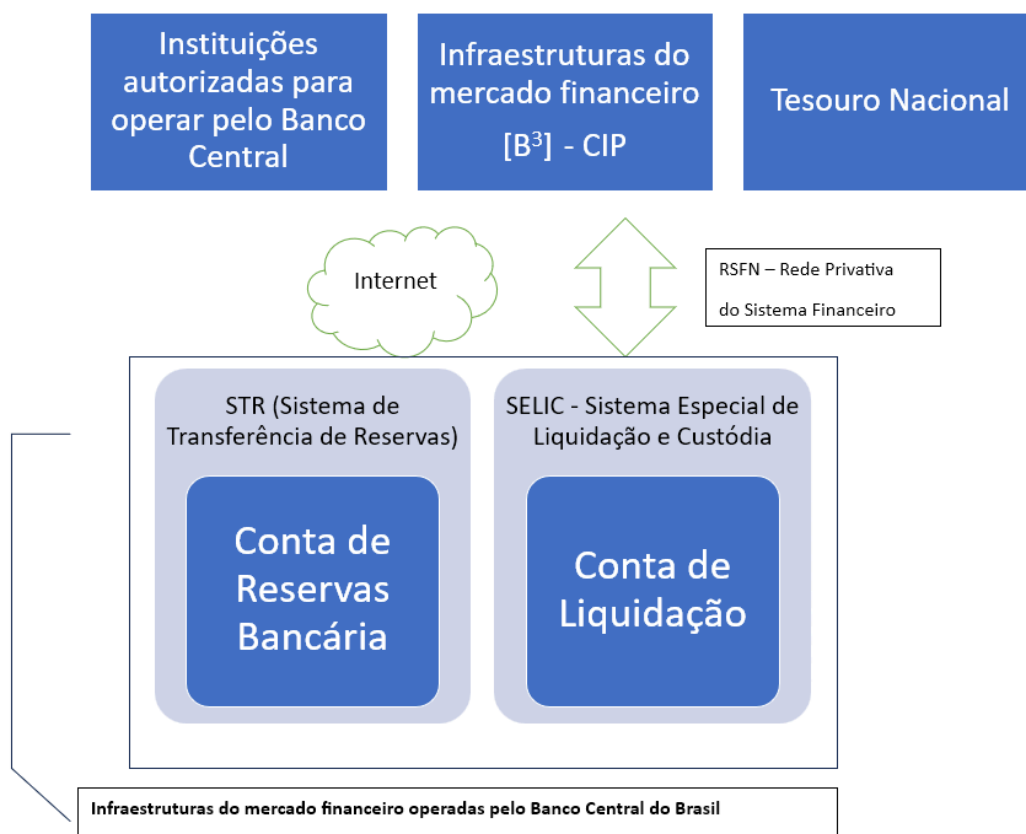


Figura 1 : Esquematização do STR

O STR opera nos dias úteis, das 06h30 às 18h30, com horários específicos para solicitação de transferências de recursos, como na (extinta) TED. Para participar do STR, as instituições financeiras o fazem por meio de Conta de Reservas Bancárias ou Conta de Liquidação. As câmaras de compensação e prestadores de serviços de liquidação usam a Conta de Liquidação para registro de movimentações financeiras.

Sistema de Pagamentos Instantâneos (SPI)

Além da Conta de Reservas Bancárias e da Conta de Liquidação, o Sistema de Pagamentos Brasileiro passou a contar, a partir de 2020 - no âmbito da implantação do sistema PIX, de um sistema de Pagamentos Instantâneo (SPI), o qual exige que as instituições

que tenham participação direta no SPI mantenham uma Conta de Pagamento Instantâneo (Conta PI), regulamentada por meio da Resolução BCB nº 195, de 2023¹⁶.

A Conta de Pagamento Instantâneo, utilizada no sistema PIX, apresenta distinções em relação às Contas de Reservas Bancárias e as Contas de Liquidação, e permite transferências imediatas e em tempo real.

Uma primeira distinção entre o STR e o STI é que este tem funcionamento durante 24 horas todos os dias do ano, enquanto o STR opera apenas em dias úteis e no horário compreendido entre 06h30 às 18h30. Além das instituições participantes diretas do SPI, há ainda participantes indiretos, que ofertam o PIX a seus clientes, mas não dispõem de Contas de Pagamentos Instantâneo, de modo que a liquidação dessas operações é executada por intermédio de uma instituição com participação direta. A regulamentação da participação dos dois tipos de instituições está consubstanciada no Capítulo IV da referida Resolução BCB 195, de 2023.

O Capítulo V normatiza a Conta PI - Conta de Pagamentos Instantâneos. A Conta PI tem alterações nos saldos mediante movimentação a crédito ou a débito, sendo que as movimentações a débito é comandada exclusivamente pelo titular da conta. Ademais, da mesma forma que as Contas de Reservas e as Contas de Liquidação, deve ser mantida com saldo maior ou igual a 0 (zero), nos termos do art. 22, §2º, da referida Resolução BCB 195, de 2023.

Sigilo bancário nas Contas de Pagamento Instantâneos

Os titulares de Contas de Pagamentos Instantâneos também têm garantias de sigilo e privacidade. O art. 16, III, garante ao titular da conta o direito de receber o “*saldo da Conta PI de sua titularidade*”, nos termos da alínea “a”); “*detalhes de um lançamento específico em sua Conta PI*”, nos termos da alínea “b”); “*relação de lançamentos em sua Conta PI no intervalo máximo de 24 (vinte e quatro) horas*”, nos termos da alínea “c”).

¹⁶ BANCO CENTRAL DO BRASIL. **Resolução BCB nº 195, de 29 de março de 2022**. Dispõe sobre os requisitos operacionais de segurança cibernética para instituições financeiras. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=195>. Acesso em: 29 ago. 2024.

Sendo assim, constata-se que, da mesma forma que as Contas de Reservas Bancárias e Contas de Liquidação, os titulares das Contas PI só têm direito de conhecer informações de saldos e transações que ocorrem na conta de sua titularidade.

Sigilo bancário e do direito à privacidade no SPB

Os tópicos anteriores mostram como os direitos ao sigilo bancário e à privacidade são implementados no âmbito das operações das instituições financeiras que participam do Sistema Financeiro Nacional no sistema interbancário operado pelo Banco Central do Brasil.

Entretanto, com o advento do PIX, e o correspondente Sistema de Pagamentos Instantâneo, o Banco Central passou a dispor e gerenciar dados informações de pessoas físicas e jurídicas não integrantes do SFN - o público em geral - ao qual também é garantido o sigilo bancário por meio da já referida da Lei Complementar nº 105, de 10 de janeiro de 2001, e a proteção e privacidade de seus dados pessoais, garantidos pela também já referida LGPD.

Os desdobramentos desses direitos nas operações do Sistema de Pagamentos Brasileiro (STR) e no Sistema de Pagamentos Instantâneos (SPI) são delineados por meio das legislações infralegais editadas pelo Banco Central do Brasil que detalharemos a seguir.

Sigilo bancário no PIX

O PIX, conforme exposto anteriormente, é um sistema de pagamentos instantâneos desenvolvido e operado pelo Banco Central do Brasil que tem uma finalidade diferenciada em relação aos demais sistemas mantidos pelo BC, nomeadamente o STR. Enquanto o STR tem a finalidade precípua de operar transferências de fundos entre instituições participantes do Sistema Financeiro Nacional, o SPI existe para permitir a liquidação instantânea de pagamentos de varejo - algo que até então o Banco Central não tinha que lidar.

Para isso, o Banco Central passou a deter informações de usuários finais, as quais estão armazenadas no Diretório Identificador de Contas Transacionais (DICT), uma plataforma tecnológica operada pelo Banco Central do Brasil. O DICT é protegido pelo sigilo bancário e pela Lei Geral de Proteção de Dados (LGPD), de modo a assegurar que as informações pessoais e financeiras dos usuários sejam mantidas confidenciais e seguras.

O delineamento desses direitos e garantias no âmbito da legislação infralegal do Banco Central, no caso do PIX, é estabelecido na Resolução BCB nº 1, de 2020¹⁷, que institui o arranjo de pagamentos Pix e aprova o seu Regulamento, e obriga, por intermédio do art. 52, I, e do art. 53, I, a todos os participantes diretos e indiretos do sistema SPI/PIX com acesso ao DICT (Diretório Identificador de Contas Transacionais), a “*zelar pela segurança e pelo sigilo das informações enviadas e obtidas por meio do DICT*”.

Além disso, o inciso VI do art. 52 da referida Resolução BCB nº 1 de 2020, determina aos participantes do sistema SPI/PIX com acesso direto ao DICT “*não utilizar, para fins comerciais, as informações obtidas a partir das ordens enviadas pelas instituições com as quais estabelecer relação para prestação de serviço de acesso ao DICT*”.

Outro aspecto que contribui para o aprimoramento do direito de privacidade no âmbito do sistema SPI/PIX é o fato de que o endereçamento das transferências de recursos é feito por meio da “chave pix”. Essa chave pode ser o número de celular, CPF/CNPJ, e-mail ou um EVP (um número aleatório gerado pelo sistema). A utilização de chaves de endereçamento simplifica o processo de transferência, eliminando a necessidade de compartilhar informações bancárias detalhadas, como número de conta e agência.

Na prática, o usuário receptor informa ao pagador apenas sua chave de endereçamento. O pagador, por sua vez, utiliza o aplicativo de sua instituição financeira ou de pagamento para inserir a chave e realizar a transação. Isso significa que os dados bancários completos não são compartilhados durante a transação, reduzindo significativamente o risco de fraude e vazamento de informações.

Sigilo bancário no SIC - Sistema de Informações ao Cidadão

O Serviço de Informações ao Cidadão (SIC), criado pela Lei nº 12.527 de 18 de novembro de 2011, conhecida como Lei de Acesso à Informação (LAI), e operacional desde 16 de maio de 2012, desempenha um papel fundamental na promoção da transparência e no acesso à informação pública no Brasil.

¹⁷ BANCO CENTRAL DO BRASIL. **Resolução BCB nº 1, de 12 de agosto de 2020**. Estabelece as condições para a autorização de funcionamento de instituições de pagamento no âmbito do SPB. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1>. Acesso em: 29 ago. 2024.

Especificamente no que se refere às informações pessoais sob custódia do Banco Central do Brasil, como o Relatório de Contas e Relacionamento (CCS), Relatório de Empréstimos e Financiamentos (SCR), Relatório de Chaves Pix, Relatório de Cheques sem Fundos (CCF) e Relatório de Câmbio, estas informações são protegidas por sigilo bancário ou pela garantia fundamental à privacidade.

O norma que regula a proteção de sigilo bancário e da privacidade e proteção desses dados no âmbito do Banco Central do Brasil é a Resolução BCB nº 287, de 2023¹⁸, a qual, em seu artigo 12 estabelece que *“toda informação tratada no âmbito do Banco Central do Brasil deve ser considerada pública, salvo as informações de acesso restrito e os dados pessoais, inclusive os sensíveis, que devem ser devidamente rotulados ou classificados de forma a indicar essa condição”*.

Além disso, o art. 17 da mesma resolução especifica que *“as áreas e instalações que contiverem informação de acesso restrito, dados pessoais ou dados pessoais sensíveis têm seu acesso limitado apenas às pessoas autorizadas”*.

Por fim, o atendimento às demandas de informação da LAI no âmbito do Banco Central do Brasil é regulado por meio da Portaria nº 98.972, de 25 de julho de 2018¹⁹, que define no art. 8 que os pedidos que versem sobre *“informação protegida por sigilo legal”* serão **indeferidos**.

CBDC - moeda digital de banco central

Após a exploração dos aspectos básicos de funcionamento do sistema financeiro nacional, e a implementação do direito à privacidade e do sigilo bancário no âmbito do SPB - Sistema de Pagamentos Brasileiro e do SPI - e do SPI - Sistema de Pagamentos Instantâneos - passamos à análise da modernização desse sistema, com a criação de uma versão digital do

¹⁸ BANCO CENTRAL DO BRASIL. **Resolução BCB nº 287, de 17 de março de 2023**. Estabelece diretrizes para a implementação de políticas de gestão de riscos e controles internos nas instituições financeiras. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=287>. Acesso em: 29 ago. 2024.

¹⁹ BANCO CENTRAL DO BRASIL. **Portaria n.º 98972, de 14 de agosto de 2023**. Disponível em: https://www.bcb.gov.br/content/acessoinformacao/normativos_ouvidoria_docs/Portarias/Portaria%2098972.pdf. Acesso em: 29 ago. 2024.

Real, no âmbito da Plataforma DREX, e os impactos dessa nova arquitetura tecnológica nos direitos ao sigilo bancário, à privacidade e à proteção de dados pessoais.

Antes, porém, de adentrarmos aos aspectos relativos ao DREX, que é o nome da moeda digital brasileira, é importante contextualizar as moedas digitais de banco central - no termo em inglês - *Central Bank Digital Currency* (CBDC), mediante a terminologia adotada pelo BIS - *Bank of International Settlements*.

O BIS conceitua²⁰ uma CBDC como “*uma nota digital. Ela poderia ser usada por indivíduos para pagar empresas, lojas ou uns aos outros (uma "CBDC de varejo"), ou entre instituições financeiras para liquidar negociações em mercados financeiros (uma "CBDC de atacado").*”

Outra definição é a adotada pelo Atlantic Council²¹ - Conselho do Atlântico Norte: “*CBDC é um dinheiro virtual lastreado e emitido por um banco central*”, sendo uma resposta dos bancos centrais à crescente digitalização dos meios de pagamento.

Segundo o Conselho do Atlântico Norte, em maio de 2024 haviam 134 países com projetos de CBDC em andamento, dos quais 3 já foram lançados: Bahamas, Jamaica e Nigéria. Em fase piloto de testes há 36 países, entre os quais do Brasil, com o DREX. A figura a seguir evidencia as diferentes fases de implementação dessas moedas digitais oficiais.

O Brasil anunciou que iria desenvolver uma moeda digital em 2017. Posteriormente, em maio de 2021, o Banco Central do Brasil (BCB) divulgou as diretrizes para o “Real Digital” (termo adotado antes da definição do nome “DREX”) simultaneamente aos aspectos prospectivos de testes para o primeiro piloto da moeda digital, o qual foi iniciado em abril de 2022. Atualmente, o DREX está em fase de testes, e tem lançamento no mercado previsto para 2025.

²⁰ BANK FOR INTERNATIONAL SETTLEMENTS. **Central Bank Digital Currencies (CBDC)**. Disponível em: <https://www.bis.org/about/bisih/topics/cbdc.htm>. Acesso em: 29 ago. 2024.

²¹ ATLANTIC COUNCIL. **Central Bank Digital Currency (CBDC) Tracker**. Disponível em: <https://www.atlanticcouncil.org/cbdctracker/>. Acesso em: 29 ago. 2024.

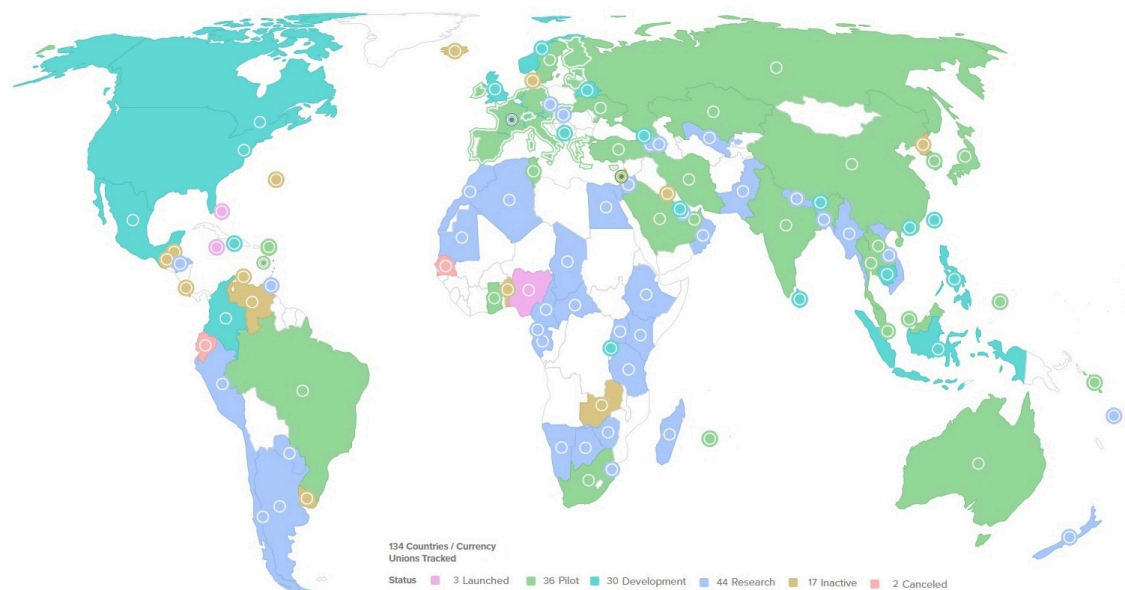


Figura 2: CBDC - fases de desenvolvimento. Fonte: *Atlantic Council CBDC Tracker*

Assim, após essa introdução ao tema CBDC, na sequência procedemos à revisão bibliográfica sobre a temática de direito de sigilo bancário, direito de privacidade em CBDCs. Posteriormente vamos explorar a arquitetura de CBDC proposta pelo BIS - *Bank of International Settlements* - com considerações sobre privacidade, e finalizamos com a análise do DREX (o Real Digital), e como ele implementa o direito ao sigilo bancário e o direito à privacidade, e se e como essa implementação atende às normas brasileiras.

CBDC - revisão bibliográfica

Nas referências bibliográficas apresentadas, diversos autores abordam temas relacionados a moedas digitais, sigilo bancário, e o papel do Estado na economia digital. Bruno Felipe de O. Miranda, em "Moeda e Direito: Elementos Para uma Teoria Constitucional", explora a relação entre moeda e direito sob uma perspectiva constitucional, focando na teoria regulatória e pública, abordando no capítulo 4, item 6 de sua obra as potenciais incompatibilidades de modelos de CBDCs com o ordenamento constitucional brasileiro.

Miranda (2022) assevera - convergindo com o pensamento de Salama e Zelmanovitz (2023) - que o art. 164 da CF88, embora não vede expressamente a criação e emissão de

CBDCs, “*alguns modelos de desenho regulatório podem implicar ofensa indireta à norma*”. O modelo de CBDC que em tese seria incompatível com a disposição constitucional seria o “CBDC de conta corrente (*account-based CBDC*)”, tendo em vista que este modelo estabeleceria uma relação direta entre o Banco Central e o público em geral, e que esse tipo de relacionamento pode configurar, mesmo que indiretamente, “algum tipo de concessão de crédito” do Banco Central para o titular da conta, o que é expressamente vedado pelo art. 164 §1º da CF88: “*É vedado ao banco central conceder, direta ou indiretamente, empréstimos ao Tesouro Nacional e a qualquer órgão ou entidade que não seja instituição financeira*”.

Nesse contexto, os óbices constitucionais à emissão de uma CBDC de varejo são: “(i) ausência de autorização constitucional específica; (ii) falta de autorização para que o BC atue no varejo; (iii) vedação constitucional à concessão de empréstimos a entidade que não seja instituição financeira”, apontando, porém, que poderiam ser superados por meio de uma emenda constitucional.

Steinberg e Espir (Steimberg, Espir, 2023) discutem a privacidade monetária e destacam a tendência histórica de governos limitarem o uso de papel moeda para mitigar a lavagem de fundos ilícitos. No Brasil, o art. 5º da CF88 e Lei Complementar nº 105, de 2001, tratam de sigilo bancário, enquanto a Lei Geral de Proteção de Dados (LGPD) abrange direitos de privacidade para além do sigilo bancário. Os autores apontam que, com o avanço de transações eletrônicas como o PIX, há uma tendência de redução da privacidade. Por outro lado, apontam que, como a maior parte das transações ocorre em moeda escritural (moeda bancária), a privacidade e o sigilo são garantidos pelas instituições financeiras ou de pagamento nos quais os cidadãos mantêm suas contas, e, em regra, são informações inacessíveis ao Banco Central.

Steinberg e Espir (Steinberg, Espir, 2023) tratam ainda dos riscos à privacidade monetária associados às Moedas Digitais de Bancos Centrais (CBDCs), dependendo do modelo utilizado, e enfatizam, que pelas regras da Lei Complementar nº 105, de 2001, o Banco Central deve respeitar as regras de sigilo. Mas os autores mostram que há limitações ao sigilo e à privacidade estabelecidas dentro da própria Lei Complementar nº 105, de 2001, em legislações relativas à lavagem de dinheiro e na Circular BCB nº 3.978, de 2020²², que

²² BANCO CENTRAL DO BRASIL. **Circular nº 3.978, de 23 de janeiro de 2020**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978>. Acesso em: 29 ago. 2024.

determina que as instituições financeiras devem reportar ao COAF, atual UIF - Unidade de Inteligência Financeira²³ - comunicação de saques ou depósitos em espécie acima de R\$ 50 mil. Os autores sustentam, portanto, que embora haja direito à privacidade e ao sigilo, ele não é irrestrito. Mas os autores salientam a importância do sigilo bancário e da privacidade para o bom funcionamento dos mercados financeiros.

Os autores (Steinberg, Espir, 2023) avançam na análise do direito à privacidade e ao sigilo no âmbito das CBDCs, que, sendo moedas digitais de curso legal, representam um passivo do Banco Central. Acrescentam que CBDCs instituídas no modelo de atacado (wCBDC), apenas o Banco Central e as instituições financeiras têm acesso a esse dinheiro, de modo que seria semelhante às atuais Contas de Reserva Bancária (reservas fracionárias) - usadas para liquidação financeira no mercado interbancário. Já uma CBDC de varejo (rCBDC) seria um modelo no qual o público em geral teria conta no Banco Central, mas como apontou Miranda (2022), há preocupações de incompatibilidade dessa arquitetura jurídica com o ordenamento constitucional vigente, especialmente o art. 164 da CF88.

Steinberg e Espir (Steinberg, Espir, 2023) apontam ainda que o formato jurídico das CBDCs também tem implicações em privacidade e sigilo. Uma CBDC em formato de conta seria semelhante à moeda escritural, consubstanciando-se em um passivo obrigacional frente a uma contraparte, enquanto uma CBDC em formato token, por ser tangível e sujeita à posse, poderia se sujeitar às regras de transmissão de propriedade dos direitos reais, por tradição, mas essa transferência requer autenticação por tecnologia de *ledger* distribuído (DLT). Os autores consideram que as mesmas regras atuais de sigilo podem ser aplicadas às CBDCs - o que desestimularia seu uso por indivíduos com intenções ilícitas.

Steinberg e Espir (Steinberg, Espir, 2023) trazem ainda a discussão o Voto-31/2023 do BCB²⁴ que determina testes de privacidade para o DREX (Real Digital) e determina aos participantes a adesão às regras da LGPD. Apontam que o DREX, no formato hoje concebido, é uma CBDC de liquidação, operada por instituições financeiras, e que levanta preocupações sobre riscos de vigilância estatal e também pelo potencial de monetização, por parte da

²³ BRASIL. Ministério da Fazenda. **Inteligência Financeira**. Disponível em: <https://www.gov.br/fazenda/pt-br/assuntos/prevencao-lavagem-dinheiro/inteligencia-financeira>. Acesso em: 29 ago. 2024.

²⁴ BANCO CENTRAL DO BRASIL. **Voto BCB nº 31, de 2023**. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/voto_bcb_31_2023.pdf. Acesso em: 29 ago. 2024.

iniciativa privada, dos dados presentes no DLT que será operado pelo BC e pelas instituições participantes.

Os autores ainda apontam que se discute a introdução de uma funcionalidade *off-line* às CBDCs o que as assemelha ao papel-moeda, e mostram que tal funcionalidade é considerada importante, mas apresenta desafios técnicos e jurídicos. Steinberg e Espir, por fim, concluem que os diferentes formatos jurídicos das CBDCs têm implicações significativas sobre sigilo e privacidade, seja CBDC de atacado ou de varejo, e se no formato token e ou conta. Importante ressaltar que o modelo do DREX é uma CBDC de atacado, *wDREX*, mas o modelo contempla ainda uma CBDC de varejo, *rCBDC*, na forma de uma *stable coin* emitida pelos bancos comerciais.

Avançando na revisão bibliográfica, Heng Wang (WANG, 2023) se debruça sobre a abordagem da China em relação à sua moeda digital centralizada, o e-CNY (Yuan Digital), tendo sido desenvolvida como uma resposta do Estado às criptomoedas privadas, as quais são vistas com potencial de afetar o próprio papel do Estado, ajudar na fuga de capitais e evitar a regulamentação. Wang sustenta que o e-CNY reflete o papel mais significativo do Estado no sistema financeiro da China relativamente a outras economias.

Heng Wang descreve o e-CNY como um CBDC de dois níveis. O PBOC - *People Bank of China*, o banco central da China - emite CBDC para instituições de segundo nível, que são instituições financeiras e PSPs (*Payment Service Provider*) - equivalentes no Brasil às Instituições de Pagamento. Estas instituições de segundo nível são as responsáveis por distribuir e-CNY para o público em geral e são também responsáveis pela conformidade à legislação antilavagem de dinheiro. O segundo nível depende da operacionalização da carteira digital e-CNY. Além desses, há um terceiro nível de operadores do E-CNY, que são bancos ou instituições de pagamento sem acesso ao sistema interbancário.

Em relação à privacidade, Heng Wang (WANG, 2023) sustenta que o e-CNY adota uma camada de anonimato gerenciado, no qual o PBOC poderá acessar dados de transações e das carteiras digitais. Por outro lado, as transações do e-CNY por meio do carteira digital transmitem apenas um identificador (ID) da carteira, o que impede que os bancos e outras partes da transação conheçam a identidade do usuário, limitando o acesso dos bancos e dos

PSPs às informações da transação. Heng Wang (WANG, 2023) conceitua o e-CNY como uma CBDC de varejo, operada em dois níveis.

Ainda em relação à privacidade, Wang assevera que a função de programabilidade do e-CNY é o que pode suscitar as maiores preocupações sobre sigilo e privacidade tendo em vista que essa função exige o acesso e tratamento de uma quantidade grande de informações, como localização, tempo, partes que estão transacionando entre outras, mas alerta que se o Banco Central falhar em garantir privacidade, os danos à reputação das moedas digitais superaram quaisquer potenciais benefícios.

Isabelle Carvalho Costa Pinto (Pinto, 2022), em sua dissertação de mestrado, oferece uma introdução geral às moedas eletrônicas de bancos centrais, e, relativamente às questões de privacidade, sustenta que o e-CNY (Yuan Digital) segue “*princípios de anonimato para transações de pequeno valor e rastreabilidade para transações de maior valor*”. Esse aspecto converge com a constatação de Steinberg e Espir (Steinberg, Espir, 2023, p 227) segundo a qual a China projeta cinco tipos de carteiras digitais para uso do público em geral, sendo as [carteiras eletrônicas] de menor importância podendo ser usadas para transações de menor valor e maior privacidade. Por outro lado, em transações de maior valor são operadas por carteiras digitais de maior sofisticação nos quais dados de identificação (KYC - *Know Your Client*) e requisitos de licitude e legitimidade da própria transação devem ser observados.

Cham (Cham, 2023) explora a diferença entre sistemas de pagamento digitais baseados em *token* (como o Bitcoin) e baseados em conta (como o Ethereum), incluindo a discussão sobre CBDCs. O autor distingue os métodos de pagamento baseados em *tokens* (por exemplo, moedas e cédulas) e sistemas de pagamento baseados em contas (por exemplo, depósitos bancários) e sustenta que os diferenciais de cada modelo estão bem estabelecidos nas discussões relativas à economia de pagamentos digitais. Conforme o autor, a diferença fundamental entre os dois tipos de arranjos reside no processo de verificação dos pagamentos. Em um sistema baseado em contas, a questão fundamental para a segurança do destinatário do pagamento é a identidade do pagador, enquanto em um sistema baseado em *tokens*, a identidade do pagador é irrelevante, e a questão crucial para o destinatário é a autenticidade do objeto recebido – se é real ou falsificado. Isso sugere que o tipo de arquitetura escolhida tem impactos nos direitos de sigilo bancário e de privacidade.

Finalmente, Gustavo Franco (FRANCO, 2020), em "O futuro do dinheiro", verifica que o propósito dos criadores da primeira moeda digital, o Bitcoin, foi o de criar um mecanismo que permite a transmissão de valores dispensando a identificação, buscando um nível de anonimato que as “*as autoridades monetárias mundo afora queriam extinguir*”.

CBDC: o modelo do BIS - Bank for International Settlements

Neste tópico exploramos o modelo de CBDC proposto pelo BIS. Entretanto, antes de entrar no detalhamento técnico, é importante explorar de forma sucinta o papel do BIS no âmbito do sistema financeiro mundial - de forma a evidenciar que é uma instituição que não tem poder regulatório sobre o Banco Central do Brasil, de modo que seus modelos propostos são indicações técnicas, que podem ou não ser seguidos pelos bancos centrais nacionais sócios do BIS, como é o caso da autoridade monetária brasileira.

BIS - aspectos regulatórios e de governança

O BIS atua²⁵ como um banco para bancos centrais, auxiliando-os e fomentando cooperação em diversas áreas de interesse, entre as quais as CBDCs - objeto de um tema de pesquisa nessa instituição. O BIS vem desenvolvendo projetos relacionados às CBDCs, incluindo provas de conceito e protótipos, os quais auxiliam os bancos centrais em suas implementações, sem que haja, porém, uma hierarquia ou vinculação regulatória ou técnica.

Nesse contexto, o BIS desenvolveu, no âmbito do Projeto Aurum²⁶, um protótipo de CBDC de dois níveis, um sistema atacado, destinado a ser usado pelos sistemas financeiros nacionais no âmbito interbancário (atacado - *wCBDC*), e uma carteira eletrônica que seria usada pelos cidadãos em suas operações com o sistema financeiro (varejo - *rCBDC*). Vamos expor seus principais aspectos a seguir.

CBDC: modelo de dois níveis do BIS

O protótipo do BIS para uma CBDC propõe uma arquitetura de dois níveis: um sistema interbancário atacadista onde a CBDC atacadista (*wCBDC* - *wholesale* CDBC) é

²⁵ BANCO CENTRAL DO BRASIL. **Banco de Compensações Internacionais (BIS)**. Disponível em: <https://www.bcb.gov.br/acessoinformacao/bis>. Acesso em: 29 ago. 2024.

²⁶ BANK FOR INTERNATIONAL SETTLEMENTS. **Project Rosalind: Exploring Retail CBDC**. Disponível em: <https://www.bis.org/about/bisih/topics/cbdc/rcbdc.htm>. Acesso em: 29 ago. 2024.

emitida pelo banco central para os bancos e demais instituições participantes do sistema financeiro de atacado, sendo esta moeda digital usada para liquidar operações entre instituições financeiras.

E, em segundo plano, um sistema de carteira eletrônica de varejo no qual uma CBDC de varejo (*r*CBDC - *retail* CBDC) é emitida pelos bancos comerciais, que por sua vez a distribui aos usuários finais, sendo esta moeda usada para os pagamentos de varejo. É importante apontar que nesse tipo de arquitetura proposta pelo BIS, a *r*CBDC, ou CBDC de varejo, equivale aos depósitos à vista nas contas do público em geral mantidos pelas instituições financeiras.

Dessa forma, a emissão da *r*CBDC ocorreria na conversão de depósitos à vista em moedas digitais, ou, alternativamente, por meio de emissão direta da *r*CBDC mediante análise de propostas de investimento - mantendo a arquitetura atual do sistema financeiro - conforme exposta Salama e Zelmanovitz (2023), que confere ao setor privado a prevalência quase absoluta na alocação de capital, ainda que sob supervisão da autoridade monetária.

De qualquer forma, o modelo de CBDC de dois níveis proposto pelo BIS procura manter os papéis institucionais vigentes dos atores dos sistemas financeiros nacionais, nos quais o Banco Central é responsável pela operação do sistema interbancário, funcionando como prestador de última instância, enquanto os bancos comerciais, instituições de pagamento operam o sistema monetário no varejo, administrando e operando os pagamentos que ocorrem entre usuários finais.

Essa arquitetura se ajusta, também, no contexto brasileiro, ao estabelecido no art. 164, §1º da CF88 - que veda ao banco central conceder, direta ou indiretamente, empréstimos ao Tesouro Nacional e a qualquer órgão ou entidade que não seja instituição financeira.

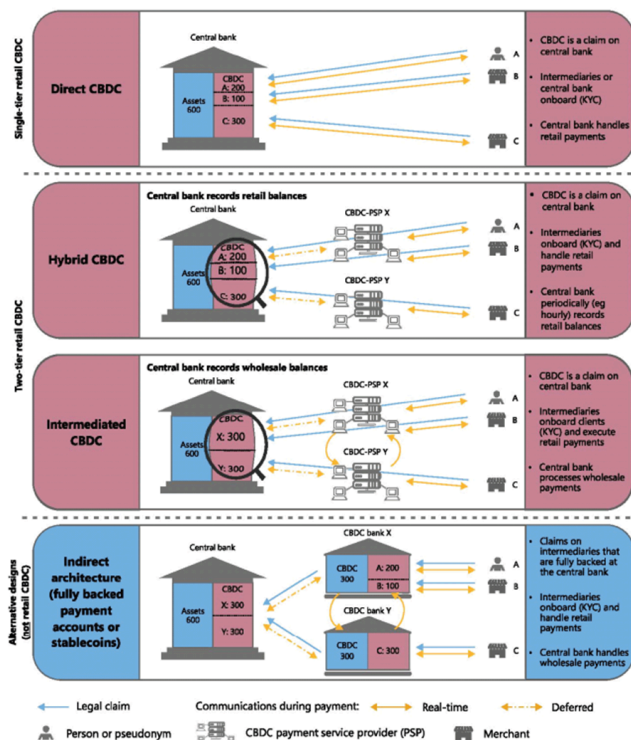


Figura 3: Arquiteturas de 2 níveis. Fonte: BIS - *A Prototype for Two-tier Central Bank Digital Currency (CBDC)*²⁷

Em termos conceituais, os tipos de CBDC de varejo (*rCBDC*) que podem ser implementados são categorizados em “diretos”, onde clientes têm suas transações registradas diretamente no livro razão digital (*blockchain*) do banco central, e “intermediados”, nos quais os clientes registram suas transações em livros razão digitais (*blockchain*) de bancos comerciais.

Entre os modelos intermediados, existem três tipos: o CBDC Híbrido, no qual o banco central mantém o controle total do livro-razão digital (*blockchain*) e a responsabilidade pela moeda digital distribuída; o CBDC Intermediado - o banco central controla apenas o livro-razão (*blockchain*) atacadista, mas ainda responsável pela moeda digital; e as Arquiteturas Indiretas, nas quais o banco central gerencia o livro-razão atacadista (*blockchain* ou *DLT*), mas o instrumento “monetário” emitido pelos bancos comerciais é comparável às

²⁷ BANK FOR INTERNATIONAL SETTLEMENTS. **BIS Innovation Hub Work Programme 2023-2024**. Disponível em: <https://www.bis.org/publ/othp57.pdf>. Acesso em: 29 ago. 2024.

moedas escriturais, dos bancos comerciais - os depósitos à vista, ou a um *e-money* ou *stablecoin*²⁸, sem constituir uma obrigação do banco central.

Sendo assim, no sistema Direct CBDC - ou CBDC de um nível, mostrado no modelo “Direct CBDC” (painel superior da Figura 2, que destacamos abaixo), o CBDC é operado diretamente no banco central, que também lida com todos os pagamentos de varejo em tempo real e, portanto, mantém um registro de direitos (créditos) de varejo.

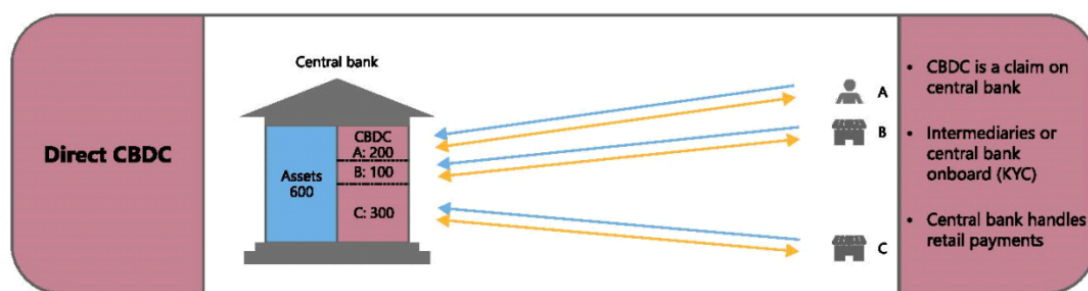


Figura 4: Modelo de CBDC Direto do BIS. Fonte: BIS - Projeto Aurum

As arquiteturas híbridas de CBDC incorporam uma estrutura de dois níveis, com direitos (créditos) diretos sobre o banco central - usados pelas instituições financeiras no sistema interbancário, enquanto os pagamentos em tempo real são gerenciados por intermediários. Há variantes dessa arquitetura híbrida. O modelo *Hybrid* CBDC, destacado na figura abaixo, o banco central pode manter uma cópia tanto das contas de atacado, quanto das contas de varejo (clientes finais).

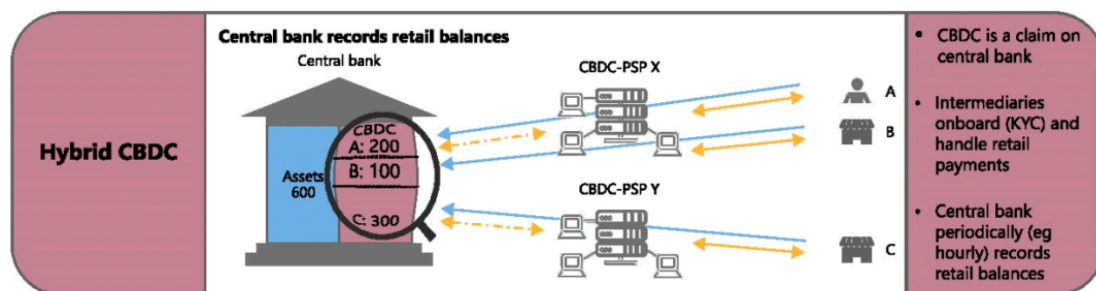


Figura 5: Modelo de CBDC Hybrid do BIS. Fonte: BIS - Projeto Aurum

²⁸ Stablecoin é uma moeda digital com lastro de uma moeda convencional, como o dólar ou o euro.

Uma outra versão do modelo híbrido de CBDC é o denominado *Intermediated* CBDC, destacado na figura abaixo, no qual o banco central armazena dados apenas dos contas de atacado (sistema interbancário).

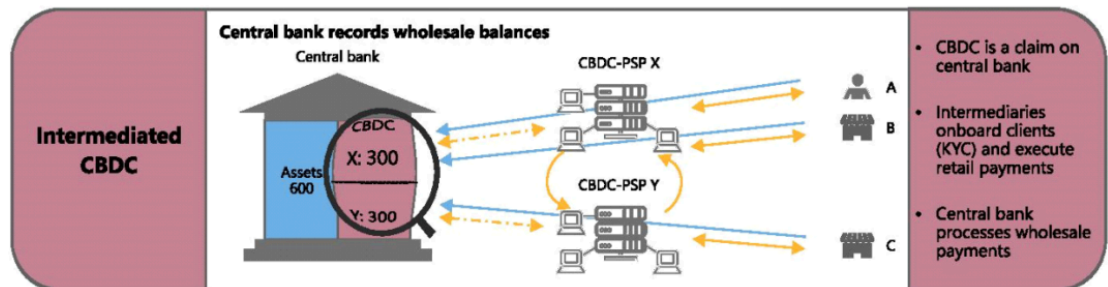


Figura 6: Modelo de CBDC Intermediated do BIS - Fonte: BIS - Projeto Aurum

Nesse modelo Intermediated, o banco central apenas administra o livro-razão digital (DLT) de atacado (terceiro painel da Figura 3). Finalmente, há o modelo de CBDC de arquitetura indireta.

Nesta última proposta de arquitetura, a CBDC é emitida e resgatada apenas pelo banco central. A CBDC circula apenas no sistema interbancário (bancos comerciais, instituições de pagamento), para liquidação de pagamentos no atacado, sendo, portanto, um *design* de uma CBDC de atacado (*wCBDC*), conforme mostrado na Figura 7 a seguir, e que tende a ser uma implementação digital criptográfica da arquitetura institucional vigente atualmente na maior parte dos países para seus sistemas financeiros, com uma separação clara entre o sistema atacadista (interbancário) e de varejo (público em geral) com prerrogativa de emissão monetária privada por parte das instituições bancárias.

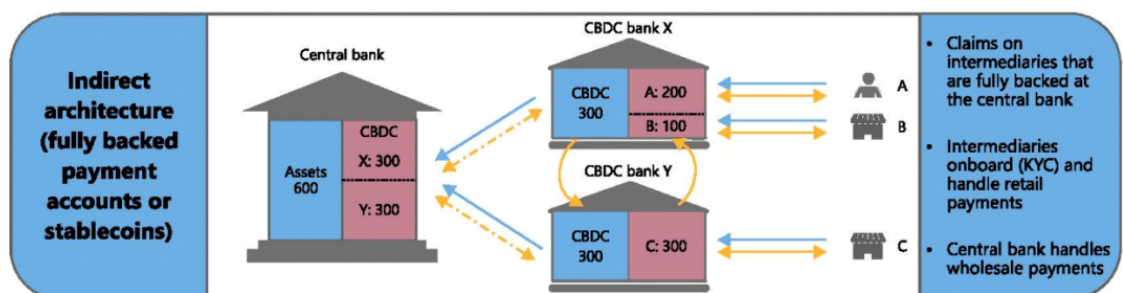


Figura 7: Modelo de CBDC Indirect do BIS - Fonte: BIS - Projeto Aurum

Dessa forma, os intermediários (bancos comerciais) emitem um direito (crédito) aos consumidores, que seria uma CBDC de varejo (r CBDC). O intermediário (banco comercial) é obrigado a lastrear total ou parcialmente cada direito de crédito (r CBDC) com uma posse respectiva de w CBDC (CBDC de atacado) - a qual representa uma “conta de reserva” no banco central. O banco central, nesses modelos intermediados, opera apenas o sistema de pagamento de atacado, assemelhando-se sua função ao que se observa atualmente nos sistemas de pagamentos mostrados por Salama e Zelmanovitz (2023) .

O nível de responsabilidade sobre os dados e a capacidade de supervisão da autoridade monetária sobre transações nas diversas arquiteturas propostas está descrito na figura a seguir (Figura 8), evidenciando um *trade-off* entre capacidade de supervisão do banco central sobre o sistema financeiro e sua responsabilidade pela guarda dos dados.

CBDC: níveis de responsabilidade do banco central em relação aos dados pessoais

Em um modelo de CBDC que o banco central opera diretamente os pagamentos de varejo, como no modelo de CBDC Direto, há uma grande responsabilidade por parte da autoridade monetária relativamente à guarda dos dados dos usuários finais do sistema de pagamento, e também baixo desacoplamento entre varejo e atacado no sistema financeiro.

Por outro lado, em um sistema *CBDC-backed stablecoin* - como o proposto pelo BIS no modelo *Indirect* CBDC - o banco central tem baixa responsabilidade sobre os dados dos usuários finais, e há uma grande divisão entre o sistema financeiro de varejo (usado pelo público em geral) e de atacado (sistema interbancário).

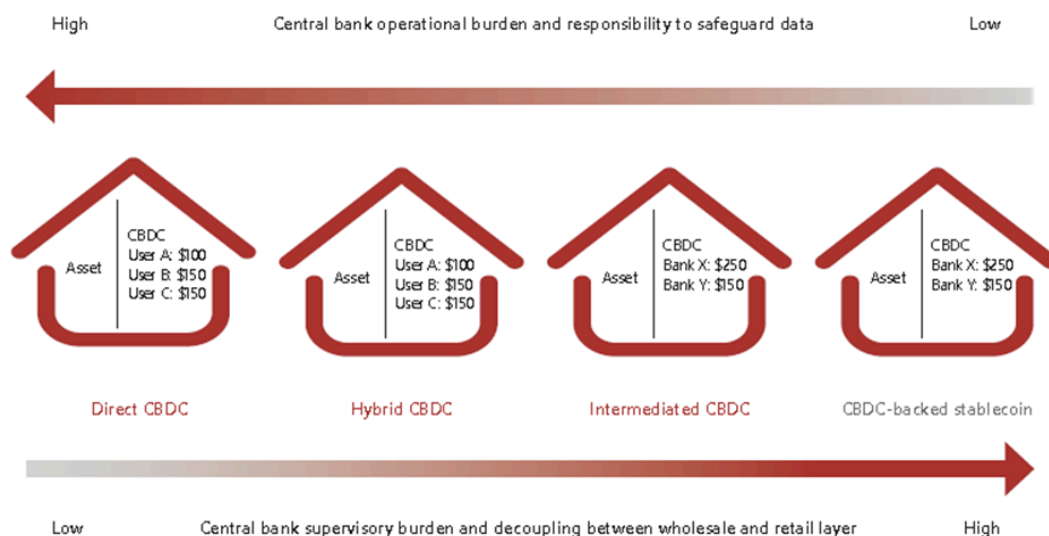


Figura 8 - Níveis de privacidade e segurança de transações de CBDC. Fonte: BIS - *A Prototype for Two-tier Central Bank Digital Currency (CBDC)*.

O protótipo do BIS, no âmbito do Projeto Aurum, optou por se concentrar na concepção nos dois conceitos mais descentralizados, o *Intermediated CBDC* (também denominado *CBDC-token*) e o *Indirect CBDC* (também denominado *CBDC-backed stablecoin*). O modelo *CBDC-token* se justifica em face de os bancos centrais pretenderem manter o setor privado como responsável pelos pagamentos e a intermediação financeira. Já o *CBDC-backed stablecoin* não é exatamente um CBDC tendo em vista que a moeda em mãos dos usuários finais não constitui um direito sobre o banco central, mas sim um direito sobre os bancos comerciais emissores da *CBDC-backed stablecoin*. Esse modelo, porém, se aproxima do sistema monetário usado pelos principais países, entre os quais o Brasil e também pelo Banco Central de Hong Kong - o qual foi parceiro do BIS no desenvolvimento do projeto Aurum.

Como veremos no tópico específico, a arquitetura escolhida pelo Banco Central do Brasil se amolda ao modelo de *CBDC-backed stablecoin* do BIS, caracterizado por dissociação elevada entre a contabilidade das transações de varejo e de atacado, o que, segundo o BIS, aumenta a segurança cibernética do sistema como um todo.

Ademais, nesse modelo *CBDC-backed stablecoin* o Banco Central tem menor carga de responsabilidade de garantia de segurança dos dados dos usuários finais, mas exige um

nível elevado de confiabilidade dos bancos comerciais, e, conseqüentemente, maior carga de supervisão do Banco Central sobre o sistema.

Privacidade e sigilo no modelo de duas camadas de CBDC do BIS

O modelo proposto pelo BIS - e também usado no DREX - de separação em duas camadas, um sistema interbancário de atacado, e uma carteira eletrônica para transações de varejo, permite que apenas os intermediários - os bancos comerciais - envolvidos em uma transação de pagamento no varejo conheçam a identidade das partes envolvidas.

O Banco Central, em tese, não tem tal informação, o que aumentaria o nível de privacidade e sigilo do usuário de varejo. Ademais, é um modelo que se assemelha à arquitetura de privacidade e sigilo do sistema de pagamento do sistema de pagamentos convencional. A concepção desse sistema é apontada pelo BIS como implementação da privacidade dos usuários desde a concepção do modelo de CBDC (BIS, 2022, p10).

Entretanto, na prática, quando se analisa a questão da privacidade monetária em DLTs como o do DREX, nota-se que o anonimato da transação seria garantido por intermédio da substituição de um “identificador de identidade”, por “identificador de carteira digital” associada a essa pessoa. Ocorre que, conforme apontou Fabio Araujo - coordenador da Iniciativa Drex no Banco Central - no Congresso Brasileiro de Internet, ocorrido em 6 de junho de 2024²⁹, esse sistema de pseudo anonimização não garante o direito ao sigilo bancário e à privacidade porque as transações ficam registradas e todos os operadores do sistema com acesso do DLT do DREX tem acesso ao histórico das transações.

Em que pese as transações não serem diretamente identificáveis às pessoas, pois, como apontado, há uma substituição, no registro da transação, da identidade pessoal, pela identidade da carteira eletrônica associada àquela pessoa. A questão subjacente, porém, conforme apontado por Araújo, é que esses registros permitem a todas entidades e pessoas com acesso ao DLT analisar o comportamento (valores e datas de transações, por exemplo), e assim determinar a identidade de quem está operando com aquela carteira - violando o sigilo bancário e a direito à privacidade.

²⁹ BCB COMUNICA. **Real Digital: tudo o que você precisa saber**. YouTube, 7 jul. 2023. Disponível em: https://www.youtube.com/watch?v=JIG_I2W6A6w. Acesso em: 29 ago. 2024.

Segundo Araújo, *“isso é um problema para a privacidade”*, sobretudo no contexto de uma moeda digital operando no ambiente regulado do Banco Central, no qual todos que possuem uma carteira passaram por um processo de identificação. Assim, embora essa informação (a identidade da pessoa associada com aquela transação) não esteja disponível na rede (DLT), é possível determiná-la, analisando o comportamento da carteira.

A identificação de quem está operando as carteiras é facilitada, segundo Araújo, em carteiras com comportamento regular ou que transacionam grandes valores. Nesse sentido, o executivo sustenta que é necessário métodos para obscurecer parte das transações. Um desses métodos seria usar várias carteiras para uma pessoa, ou as chamadas *omnibus account*, que ajudam a ocultar as transações individuais e manter a privacidade dos clientes.

A estratégia de uso de várias carteiras para uma única pessoa é operada da seguinte forma. A cada transação uma carteira eletrônica associada a essa pessoa é aleatoriamente escolhida para iniciar a transação, de modo a dificultar a análise de comportamento da carteira. Uma camada adicional de proteção, segundo Fábio Araújo, seria agregar tais carteiras agregadas a uma *omnibus account* e depois redistribuídas, obscurecendo ainda mais a origem das transações. Porém, o executivo apontou que *“algumas transações podem não ser cobertas por essas técnicas”*.

Fábio Araújo asseverou, ainda, que a *“privacidade é essencial para garantir a confiança no sistema. As pessoas não vão operar em um ambiente onde suas informações financeiras podem ser expostas a qualquer momento”*, e completou que *“precisamos garantir essa privacidade para manter a confiança da população e a integridade das transações”*.

Privacidade das partes - Projeto Tourbillon do BIS

O BIS, além do projeto Aurum, desenvolveu também o “Projeto Tourbillon” - o qual é uma tentativa de responder às crescentes preocupações com a privacidade em pagamentos digitais. Em um mundo onde o uso de dinheiro físico está diminuindo e os pagamentos digitais estão se tornando cada vez mais comuns, o projeto explora como uma moeda digital de banco central (CBDC) de varejo pode oferecer anonimato semelhante ao do dinheiro físico.

O Projeto Tourbillon, conduzido pelo *BIS Innovation Hub Swiss Center*, investiga como preservar a privacidade nos pagamentos enquanto mantém o equilíbrio necessário com a segurança e a prevenção de atividades ilícitas. A privacidade é entendida como o direito de manter informações pessoais em segredo ou conhecidas apenas por um grupo confiável de pessoas. Isso é especialmente relevante em transações financeiras, onde a privacidade é uma preocupação crescente.

Atualmente, a privacidade nos pagamentos assume várias formas. O dinheiro físico oferece total anonimato, mas não pode ser usado *online*. Cartões de crédito e débito envolvem o compartilhamento de dados com empresas, que são confiadas para manter a confidencialidade. As criptomoedas oferecem certo nível de anonimato, mas todas as transações são públicas. O Projeto Tourbillon busca uma nova abordagem: o “anonimato do pagador”.

Anonimato do Pagador

O Projeto Tourbillon propõe que os consumidores (pagadores) tenham anonimato semelhante ao usufruído quando transacionam com dinheiro físico, o que significa que a identidade do consumidor não pode ser vinculada à sua transação. No entanto, a identidade de quem está recebendo os recursos fica registrada na transação, e é visível ao banco comercial ao qual o recebedor está vinculado. O banco central não vê as identidades do pagador ou do recebedor, criando equilíbrio entre privacidade e a necessidade de combater atividades ilícitas. Entretanto, mediante decisões judiciais, o sigilo pode ser quebrado de modo que o banco comercial forneça os dados do recebedor no âmbito de procedimentos inquisitórios ou judiciais de combate a operações financeiras ilícitas.

O projeto concluiu que é viável construir um protótipo que garanta anonimato do pagador, segurança e escalabilidade, e que é capaz de processar cerca de 2,5 mil transações por segundo, com tempos de autenticação em torno de 1 segundo. Entretanto, quando o projeto testou um protótipo que implementa criptografia que mantém a segurança do sistema frente a ataques provenientes de eventuais sistemas baseados em computação quântica, a performance, o tempo de autenticação subiu para valores superiores a 5 segundos, e a capacidade de processamento caiu para entre 11 e 20 transações por segundo.

CBDC - aspectos ambientais

Um outro aspecto que vem sendo debatido no âmbito das moedas digitais - especialmente as moedas digitais privadas - é a questão do excessivo consumo de energia elétrica consumido pelas redes que lhes dão suporte existencial, especialmente o Bitcoin.

O documento do BIS para o Projeto Aurum enfrenta essa questão e estabelece que o modelo Aurum de dois níveis de CBDC³⁰, conforme dados da *Cambridge Centre for Alternative Finance and Statista*, o CBDC baseado nesse protótipo do Projeto Aurum teria uma pegada de carbono de 0,00110 gCO₂. Para efeito de comparação, segundo o mesmo documento, o Bitcoin teria emitido em 2021 um volume de 600.000 gCO₂.

DREX - CBDC do Brasil

Após a análise dos modelos de CBDC propostos pelo BIS, iniciamos a análise da implementação da CBDC brasileira. O interesse crescente em moedas digitais de banco central (CBDC) tem levado vários bancos centrais - incluindo o Banco Central do Brasil - a estudar, explorar e testar sistemas de CBDC. Essas moedas digitais prometem aumentar a eficiência dos serviços financeiros e de pagamentos de varejo, além de fomentar a competição e a inclusão financeira, especialmente para aqueles com acesso limitado ou inexistente a serviços bancários.

O Banco Central do Brasil, atento a essa tendência desde 2017, formou um Grupo de Trabalho dedicado a estudar a emissão da moeda digital brasileira, inicialmente denominada Real Digital, e, posteriormente, DREX. As conclusões desse grupo e as discussões subsequentes culminaram na definição das "Diretrizes do Real Digital" em maio de 2021, atualizadas em fevereiro de 2023³¹, e na organização de webinários e desafios de inovação para explorar aplicações potenciais do DREX.

Conforme a Resolução BCB nº 315, de 27 de abril de 2023, foi criado, no âmbito do Banco Central do Brasil, o Comitê Executivo de Gestão do Projeto-Piloto da Plataforma do Real Digital, o qual, posteriormente, com a definição oficial no nome da moeda digital

³⁰ BANK FOR INTERNATIONAL SETTLEMENTS. **BIS Innovation Hub Work Programme 2023-2024**. Disponível em: <https://www.bis.org/publ/othp57.pdf>. Acesso em: 29 ago. 2024.

³¹ BANCO CENTRAL DO BRASIL. **Banco Central divulga regulamento do Real Digital**. 16 maio 2023. Disponível em: <https://www.bcb.gov.br/detalhenoticia/667/noticia>. Acesso em: 29 ago. 2024.

brasileira, foi alterada pela Projeto-Piloto da Plataforma DREX, denominada Piloto Drex. Esta iniciativa buscou validar o uso de tecnologia de registro distribuído (DLT), para a emissão do Real Digital, sem envolver transações reais, através de uma colaboração entre participantes selecionados.

O Projeto-Piloto da Plataforma do Real Digital, sob a referida Resolução BCB nº 315, de 2023, estabelece uma infraestrutura de teste baseada na Tecnologia de Registro Distribuído (DLT) utilizando a plataforma *Hyperledger Besu*, compatível com a Ethereum Virtual Machine (EVM). O foco do projeto é validar a aplicabilidade da tecnologia DLT para a emissão de moeda digital, garantindo a observância dos requisitos legais e regulatórios, especialmente no que tange à *privacidade das informações de indivíduos*.

Conceito - Tecnologia DLT - Registro Digital Distribuído

Antes de expor a arquitetura da Plataforma DREX, exploramos conceitos e tecnologias nos quais essa plataforma é estabelecida, iniciando pelo DLT - *Digital Ledger Technology*. Conforme Bech e Garrat (Bech, Garrat, 2017), a tecnologia de registro distribuído (DLT - *Distributed ledger technology*) refere-se aos protocolos e infraestrutura que permitem que computadores em diferentes locais proponham e validem transações e atualizem registros de forma sincronizada em uma rede, sem a necessidade de uma autoridade central. Segundo os autores, em um banco de dados distribuído tradicional, um administrador desempenha a função de manter a consistência entre as várias cópias do registro, mantendo uma cópia principal que é periodicamente atualizada e compartilhada com todos os participantes.

Por outro lado, segundo Bech e Garrat (Bech, Garrat, 2017, Box A), os novos sistemas monetários privados baseados em DLT, como o Bitcoin e o Ethereum, são projetados para manter o registros públicos descentralizados, autênticos e confiáveis, sem a necessidade de recorrer a uma autoridade confiável. Como esses recursos são organizados em blocos sequenciais conectados em cadeia, esse tipo de DLT é chamado de "tecnologia *blockchain*", ou simplesmente "*blockchain*".

A tecnologia DLT, posteriormente, passou a ser vista com potencial de aplicação em diversos campos, entre os quais versões digitais das moedas nacionais, propiciando modelos

de negócios que respondem à crescente demanda por métodos de pagamento digitalmente nativos. Ademais, a tecnologia DLT também promete redução de custos por meio de automação e programabilidade, e capacidade de se agregar às transações monetárias contratos inteligentes (*smart contracts*) que executam transações automaticamente quando condições predefinidas são cumpridas.

O Banco Central do Brasil, em seu Relatório de Estabilidade Bancária de 2023, no documento “*Real Digital: uma plataforma para as finanças “tokenizadas”*”³² (Banco Central do Brasil, 2023), constatou uma lacuna na infraestrutura financeira atual: ante a ausência de uma moeda emitida por Banco Central que seja compatível com o ambiente DLT e com transações envolvendo ativos digitais, ou “*tokens*”, surgiram no mercado moedas digitais de emissão privada, conhecidas como *stablecoins*, que são usadas para liquidação financeira dessas transações digitais, muitas vezes sem a regulação adequada, o que pode, segundo o documento, “comprometer a estabilidade financeira”.

Nesse contexto, a implementação de uma infraestrutura DLT para o DREX visa, segundo o Banco Central do Brasil, superar essas limitações. Ela promete um alto grau de auditabilidade, rastreabilidade e transparência, fornecendo as ferramentas necessárias para uma eficaz supervisão e regulação. Ao adotar tais tecnologias com o Drex, o Banco Central sustenta que os benefícios serão estendidos a uma base mais ampla de cidadãos, garantindo-lhes acesso a serviços financeiros inovadores e seguros sem os riscos associados a um ambiente financeiro não regulamentado, como é o caso das moedas digitais privadas.

DLT baseado em conta - questões de privacidade e sigilo

Akcora, Gel e Kantarcioglu (Akcora; Gel; Kantarcioglu, 2021) exploram os dois principais tipos de contabilização de *blockchains* (DLTs) que são usados em moedas digitais: DLT baseados em conta, como o adotado pela Plataforma Ethereum, e também pela Plataforma DREX, e os baseados baseados em UTXO (*Unspent Transaction Output*), que é adotado pelo Bitcoin.

³²BANCO CENTRAL DO BRASIL. **Relatório de Economia Bancária 2022 - Boxe 9: Pagamentos instantâneos no Brasil: o PIX.** Disponível em: https://www.bcb.gov.br/content/publicacoes/boxe_relatorio_de_economia_bancaria/reb2022b9p.pdf. Acesso em: 29 ago. 2024.

O tema já foi abordado na revisão bibliográfica (Cham, 2023), no qual o autor trata o modelo baseado em UTXO como “token”. O tema é importante pois o tipo de escolha de arquitetura de DLT (conta ou UTXO) tem implicações diretas no nível de privacidade e sigilo das transações.

Akcora, Gel e Kantarcioglu (Akcora; Gel; Kantarcioglu, 2021) mostram que a diferença entre esses modelos impacta significativamente as redes *blockchain*. Nos *blockchains* baseados em conta, cada usuário tem uma conta na rede associada a si, e esse usuário pode gastar parte de suas moedas digitais e manter o saldo restante - um funcionamento semelhante a uma conta bancária. Nesse modelo, as transações têm um endereço eletrônico de entrada e um de saída, e os endereços eletrônicos podem ser reutilizados, ou seja, cada usuário da rede adota apenas um endereço eletrônico - que não necessariamente o identifica.

Entretanto, como os endereços eletrônicos nesses DLT baseados em contas - como o do Ethereum e do DREX - vão sendo reutilizados, é possível utilizar mecanismos como os usados para analisar comportamento de perfis de redes sociais para determinar o comportamento daquele perfil e com isso associar a identidade da pessoa que controla aquele endereço (que seria como um perfil da rede social).

Em contraste, os *blockchains* baseados em UTXO, como Bitcoin, utilizam endereços de uso único. Isso significa que a cada transação monetária em uma rede como a do Bitcoin, o usuário terá um endereço eletrônico diferente. Isso dificulta a análise de rede e de perfis para determinar comportamentos e, ao final, identificar as pessoas que controlam determinados endereços na rede.

Os autores (Akcora; Gel; Kantarcioglu, 2021) mostram que o termo “Plataforma” é usado para DLTs (*blockchains*) baseados em conta, porque esses DLTs permitem que sejam rodados contratos inteligentes (*smart contracts*), que são necessários para implementar modelos de negócios diferenciados. Já os DLTs baseados em UTXO servem apenas para transferência monetária.

Conceito - DeFi - Finanças Descentralizadas

O Banco Central do Brasil (Banco Central do Brasil, 2023, p170) relatou que o modelo inspirador para o DREX foi o proposto por Schär 2021³³ para um ecossistema de finanças descentralizadas (DeFi) construído sobre a *blockchain* da rede Ethereum³⁴, dividido em camadas dedicadas: à liquidação; ao registro de ativos; aos protocolos de negociação; à oferta modular de serviços financeiros – aplicações; e à agregação desses serviços.

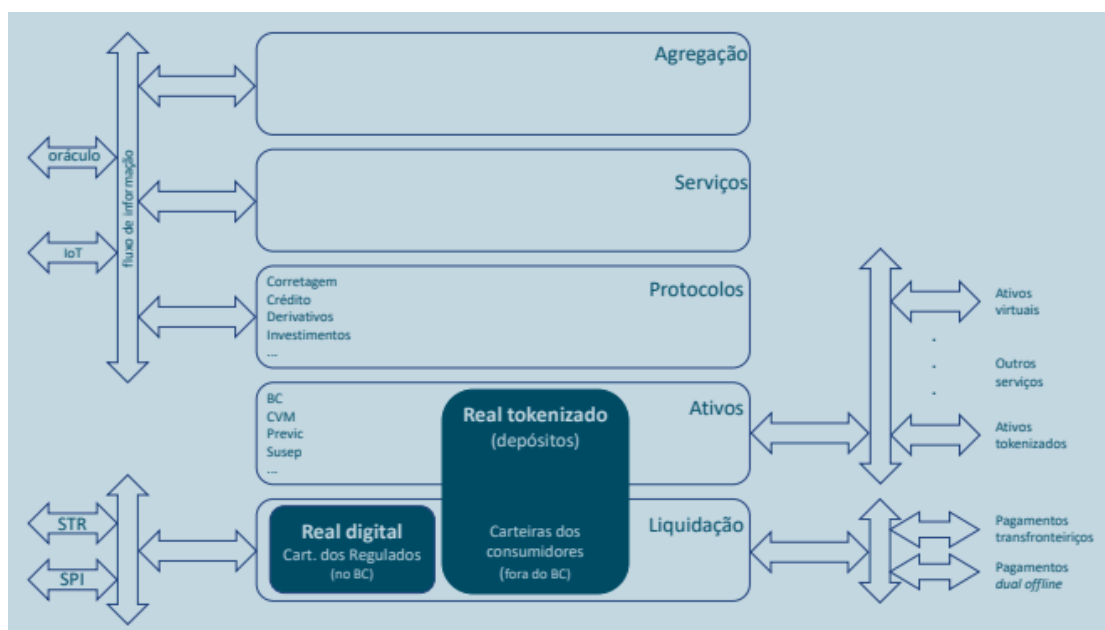


Figura 9: Plataforma do Real Digital. Fonte: (Banco Central do Brasil, 2023, p172)³⁵

Conforme pode ser visto na esquematização proposta na Figura 9, há duas versões do Real Digital, o Real Digital propriamente dito (*w*DREX), usado exclusivamente pelas instituições financeiras e em sua relação com o Banco Central, e com os demais sistemas interbancários, o STR e o SPI. Há ainda o Real Tokenizado (*r*DREX), que é a versão digital dos depósitos bancários, para ser usado pelo público em geral.

³³ SCHÄR, Fabian. **Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets**. Federal Reserve Bank of St. Louis Review, v. 103, n. 2, p. 153-174, 2021. Disponível em: <https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets>. Acesso em: 29 ago. 2024.

³⁴ ETHEREUM FOUNDATION. **Ethereum**. Disponível em: <https://ethereum.org/pt-br/>. Acesso em: 29 ago. 2024.

³⁵ BANCO CENTRAL DO BRASIL. **Relatório de Economia Bancária 2022 - Boxe 9: Pagamentos instantâneos no Brasil: o PIX**. Disponível em: https://www.bcb.gov.br/content/publicacoes/boxe_relatorio_de_economia_bancaria/reb2022b9p.pdf. Acesso em: 29 ago. 2024.

Nesse contexto, o Banco Central seria responsável por desenvolver e gerenciar as camadas de liquidação e de registro de ativos, e a definição de protocolos básicos. As camadas de serviços e de agregação seriam implementadas por sistemas dos bancos comerciais ou parceiros segundo o modelo regulatório da autoridade monetária.

DREX - Diretrizes de projeto

As diretrizes de projeto do DREX emitidas em 2021 foram atualizadas em 2023, e delineiam uma abordagem que enfatiza a integração de tecnologias de *blockchain* (registros descentralizados), contratos inteligentes e dinheiro programável, e a compatibilidade com operações através da "internet das coisas" (IoT). Elas visam o desenvolvimento de aplicações online, com possibilidade de transações offline, e a emissão de Drex de atacado (*wDREX*) pelo Banco Central, promovendo serviços financeiros de varejo liquidados pelo Drex de varejo (*rDREX*) emitido por participantes do Sistema Financeiro Nacional (SFN) e do Sistema de Pagamentos Brasileiro (SPB).

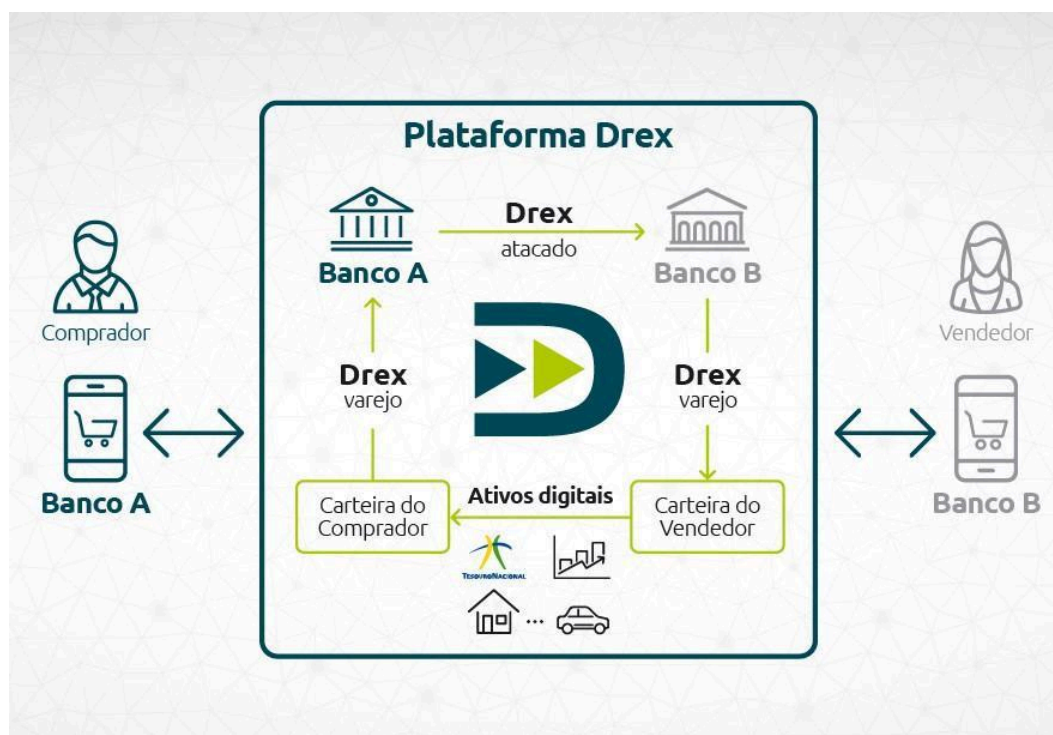


Figura 10: estrutura básica do DREX - Fonte: BCB³⁶

³⁶ BANCO CENTRAL DO BRASIL. **Drex: a moeda digital do Banco Central do Brasil**. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/drex>. Acesso em: 29 ago. 2024.

Ademais, o BCB estabeleceu como uma das diretrizes a compatibilidade do DREX com as transações com ativos tokenizados. E, ainda, que a moeda de liquidação no sistema interbancário (*w*DREX), o DREX de atacado seria uma versão digital das Contas de Reservas ou das Contas de Liquidação. Segundo o Banco Central, essa nova arquitetura disponibilizaria um ambiente propício para inovações pelos diversos agentes do mercado financeiro.

A arquitetura de dois níveis do DREX

As diretrizes finais do DREX definiram que a implementação do Real Digital mantém a intermediação financeira e a capacidade de alavancagem e de geração de crédito do sistema bancário. Além disso, as instituições autorizadas pelo Banco Central do Brasil emitem as moedas digitais *r*DREX para os clientes finais, pessoas naturais e pessoas jurídicas não financeiras.

No que respeita à privacidade, o DREX deve observância aos princípios e regras de sigilo e privacidade previstos na legislação brasileira, em especial na Lei Complementar nº 105, de 10 de janeiro de 2001 (Sigilo Bancário), e na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

Além disso, as diretrizes enfatizam a aplicação de normas e regras atuais, a garantia de segurança jurídica, e o respeito aos princípios de privacidade e segurança. O design tecnológico do Drex, segundo as diretrizes do Banco Central, visa atender integralmente às recomendações internacionais e às normas legais sobre prevenção à lavagem de dinheiro e ao financiamento do terrorismo, além de permitir o rastreamento de operações ilícitas por ordens judiciais.

DREX de atacado e DREX de varejo

Como já abordamos previamente neste trabalho, a arquitetura do sistema DREX estabelecida pelo Banco Central do Brasil é de duas instâncias: DREX de varejo (*r*DREX), para ser usado pelo público em geral, e DREX de atacado (*w*DREX) para o sistema interbancário. A implementação dessa arquitetura envolve três componentes principais: a própria Plataforma Drex, o Drex de Atacado (*w*DREX - correspondente ao *w*CBDC no modelo do BIS) e o Drex de Varejo (*r*DREX - *r*CDBC no modelo do BIS). Cada um desses

elementos desempenha um papel no funcionamento e na utilidade do sistema, refletindo a visão do Banco Central para a modernização do sistema financeiro através da tecnologia DLT.

O *w*DREX será uma moeda operada no atacado (*w*CDBC) pelas instituições financeiras e instituições de pagamento, operando versões digitais das Contas de Reserva (dos bancos comerciais), Contas de Liquidação (das instituições de pagamento). O DREX de varejo (*r*DREX) é a versão digital dos depósitos bancários à vista (dos bancos comerciais) e da moeda eletrônica (das instituições de pagamento), e seria disponibilizado ao público em geral, visando à massificação dos benefícios da tecnologia DLT para os clientes finais do SFN e do SPB.

Os clientes finais terão acesso à infraestrutura DREX por meio de seus relacionamentos com as instituições financeiras e de pagamentos, utilizando o *r*DREX (DREX de varejo), que é uma *stable coin*, que representa um direito contra o banco comercial.

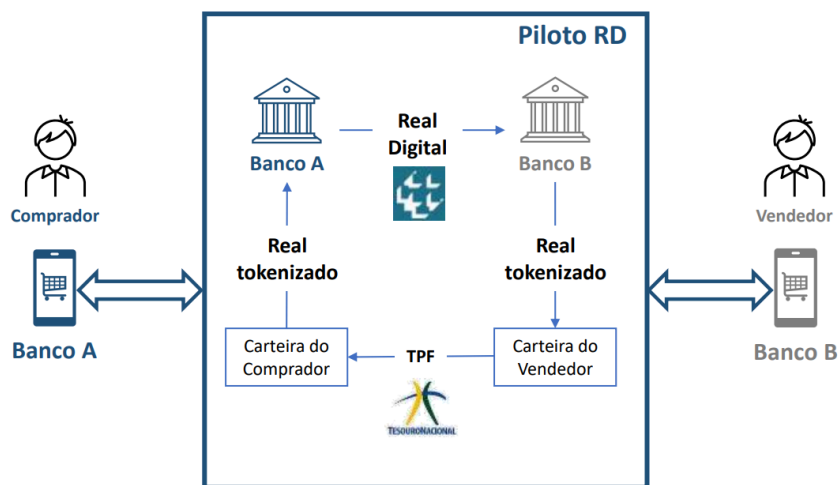


Figura 11: transação no Drex - fonte: BCB³⁷

³⁷ BANCO CENTRAL DO BRASIL. **Workshop Sessão 2: Modelos de Negócio - Piloto Real Digital**. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/workshop/Workshop_Sessao_2_Modelo_sDeNegocio_Piloto_RD.pdf. Acesso em: 29 ago. 2024.

O processo mostrado na figura acima ilustra uma transação simulada no ambiente do DREX envolvendo a compra e venda de títulos públicos por meio de um aplicativo bancário integrado.

Convergindo com o conceito do BIS, o *rDREX* é a uma *backed-stable coin*, tendo em vista que seu valor é estável (*stable*) e é garantida (*backed*) por uma correspondência em *wDREX*, parcial ou total, mantida pelo emissor (banco comercial) no Banco Central. O *rDREX* permite funcionalidades de programabilidade disponíveis na Plataforma DREX. Tal proposta permite que os clientes finais tenham acesso a serviços e ao mercado de ativos tokenizados, ao passo que preserva a estrutura de intermediação atual do SFN.

Ainda segundo o Banco Central do Brasil, a divisão do DREX em "atacado" (para transações entre bancos) e "varejo" (para uso diário pela população) permite que se transforme depósitos à vista convencionais em formato digital, visando uma transição suave entre as finanças convencionais e digitais. A longo prazo, segundo o BCB, o objetivo é alcançar um "*ledger unificado*".

DREX - DLT unificado

O Banco Central do Brasil está desenvolvendo também um "*Ledger Unificado*" para o sistema financeiro nacional, conforme destacado no relatório do *Bank of International Settlements* (BIS). Esse conceito, segundo o BCB, não se refere a uma arquitetura física única, mas sim a uma abordagem lógica de unificação onde diferentes *blockchains* podem operar de forma coesa e interoperável. O objetivo, segundo o Banco Central, é criar um ambiente onde transações e ativos possam ser gerenciados de maneira eficiente, segura e integrada.

Transição para o *Ledger Unificado*

A transição para um ambiente de Ledger Unificado envolverá a convergência gradual de várias *blockchains* à medida que as tecnologias de interoperabilidade se fortalecem. Inicialmente, pode ser necessário concentrar os ativos mais relevantes e sensíveis em uma única *blockchain* controlada pelo sistema financeiro nacional, especialmente se a interoperabilidade entre as redes ainda não for suficientemente forte ou segura. Isso garantiria a segurança e a integridade das transações mais críticas.

DREX - DLT do Real Digital de Atacado (wDREX) - Hyperledger Besu

A Plataforma DREX é a espinha dorsal do sistema, a infraestrutura sobre a qual todas as transações e interações são realizadas. O ponto central da Plataforma DREX é o sistema *Hyperledger Besu*, escolhido para piloto do Real Digital, sendo compatível com o Ethereum Virtual Machine (EVM), o que permite à plataforma suportar aplicações e contratos inteligentes (*smart contracts*) desenvolvidos para o ecossistema Ethereum.

O Hyperledger Besu permite a implementação de um DLT permissionado, no qual o acesso é restrito e controlado, como é o caso da Plataforma DREX, que apenas o Banco Central e instituições que participam do Sistema Financeiro Nacional têm acesso.

Em relação ao sistema de autenticação das transações, o sistema escolhido pelo Banco Central do Brasil para o DREX é o *Proof of Authority (PoA)* - um algoritmo de consenso utilizado em redes *blockchain* onde os participantes são conhecidos e confiáveis. Esses validadores de transações são instituições autorizadas previamente pelo Banco Central do Brasil e são responsáveis por verificar as transações e incluí-las nos blocos do DLT, formando a cadeia de blocos (*blockchain*).

Hyperledger Besu e Ethereum Virtual Machine (EVM)

O *Hyperledger Besu* é o sistema central da Plataforma DREX e ele opera um sistema que é compatível com a rede Ethereum, tendo em vista que adota o Ethereum Virtual Machine (EVM). Com essa escolha tecnológica, a Plataforma DREX tem a funcionalidade de programabilidade da moeda, e é um componente de software que executa os contratos inteligentes.

A escolha desses sistemas - o Hyperledger Besu e sua compatibilidade com a Ethereum Virtual Machine está juridicamente estabelecida por meio do art. 3º do REGULAMENTO DO PROJETO-PILOTO DA PLATAFORMA DO REAL DIGITAL, ANEXO II À RESOLUÇÃO BCB Nº 315, DE 27 DE ABRIL DE 2023:

*“Art. 3º O Piloto RD tem por objetivo validar o uso de uma solução de Tecnologia de Registro Distribuído (DLT), na plataforma **Hyperledger Besu**, avaliando a programabilidade com ativos financeiros e a capacidade de observância aos requisitos legais e regulatórios,*

principalmente em relação à privacidade das informações de indivíduos e demais envolvidos nas transações na plataforma do Real Digital, bem como sua viabilidade tecnológica.”

Ethereum Virtual Machine - considerações sobre privacidade e sigilo

BUELAU e SANTOS (2023) sustentam que o uso da Ethereum Virtual Machine (EVM) para blockchains permissionadas, como a que está sendo implementada pelo Banco Central do Brasil, apresenta desafios - especialmente na área de privacidade. Segundo os autores, esses DLTs funcionam com base em contas, permitindo que todos os validadores na rede DLT tenham acesso a todos os dados armazenados no *blockchain*, o que os tornam particularmente problemáticos para instituições financeiras que atuam como validadores, pois elas podem potencialmente visualizar transações e informações de contas de outras instituições. Tal exposição compromete a confidencialidade e pode erodir a confiança entre os participantes, afetando a segurança geral da rede.

Os autores BUELAU e SANTOS (2023) relacionam algumas medidas que podem ser usadas para garantir a privacidade em blockchains permissionados baseados em EVM, e seriam as seguintes: criptografar os dados no blockchain; regular os validadores para restringir o acesso a certos dados; usar múltiplas blockchains privadas, permitindo que cada instituição financeira seja o único validador de sua própria blockchain.

Em seu artigo, BUELAU e SANTOS (2023) concluem que a solução ideal seria manter os dados privados confinados dentro de cada instituição financeira, em uma sistemática que é similar ao conceito do atual SPB. Ou seja, advogam pela solução de múltiplas *blockchains* privadas, uma para cada instituição financeira ou validadora, melhorando o controle sobre os dados e reduzindo riscos de acessos não autorizados.

Para tentar endereçar essas questões de insuficiência de privacidade e de sigilo associados com a escolha da Hyperledger Besu e a Ethereum Virtual Machine, o Banco Central estabeleceu testes com sistemas que implementam um conceito tecnológico denominado ZKP - *Zero Knowledge Proof*.

A tecnologia de "Zero Knowledge Proof" (ZKP), ou Prova de Conhecimento Zero, é um método criptográfico que permite a uma parte provar a outra que possui uma determinada

informação, sem revelar qual é essa informação. Este conceito está presente nos sistemas que vêm sendo testados pelo Banco Central do Brasil, os seguintes.

Anonymous Zether

O “Anonymous Zether” é evolução nas plataformas de contratos inteligentes baseadas em *blockchain*, como o Ethereum. Ele propõe um mecanismo de pagamento totalmente descentralizado e confidencial, compatível com Ethereum, e adota uma arquitetura baseada em contas. O que distingue o Zether é o fato de manter os saldos das contas criptografados.

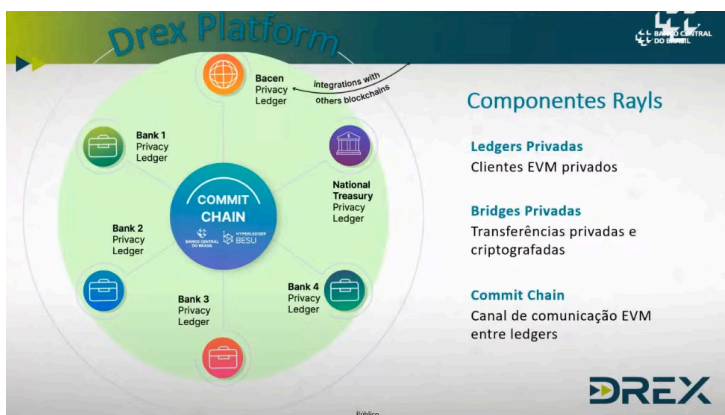
Starlight

O Starlight é outra solução que está sendo testada pelo Banco Central no projeto do DREX para garantir privacidade. A tecnologia utiliza o protocolo de *Zero-Knowledge Proof* (ZKP), que permitiria, em tese, que um indivíduo comprove que possui saldo suficiente para realizar uma transação sem ter que exibir o montante.

O Starlight também seria capaz de mascarar informações transacionais sensíveis de contratos inteligentes em *blockchains*.

Rayls - Parchain

A Parchain é uma empresa brasileira no setor de ativos digitais, que desenvolveu uma *blockchain* permissionada especializada para atender às necessidades do setor financeiro. Esta *blockchain* é apontada por dispor de compatibilidade com a tecnologia que está sendo explorada nos testes do DREX.



DREX - Considerações sobre privacidade

A Plataforma DREX, por se tratar da representação em uma rede DLT dos depósitos em IFs (Instituições Financeira) ou em IPs (Instituições de Pagamento), herda o correspondente regime jurídico quanto ao acesso e ao trânsito de informações do Sistema de Pagamentos Brasileiro.

Herda, também, todos os requisitos estabelecidos em nível constitucional, legal e infralegal relativos ao sigilo bancário e à proteção à privacidade e aos dados das pessoas envolvidas nas transações.

Teoria da privacidade - Integridade contextual no âmbito de CBDCs

Nesse contexto é necessário analisar como os direitos de privacidade podem ser garantidos na nova tecnologia. Retomando Jiang (2023), a teoria da integridade contextual da privacidade é adequada no contexto da Moeda Digital de Banco Central (CBDC), que introduz novos desafios, como a necessidade de equilibrar a autonomia financeira individual com questões de segurança nacional (combate às atividades financeiras ilícitas).

A teoria da integridade contextual se adapta às necessidades dos CBDCs porque pode abranger a complexidade e as nuances das questões de privacidade que surgem com diferentes designs de sistemas de CBDC, sejam eles centralizados ou baseados em tecnologia de livro-razão distribuído (DLT). Diferentes estruturas permitem que múltiplos atores, como bancos centrais, comerciais, e outras entidades autorizadas, colem, acessem e armazenem dados de maneiras - o que levanta questões únicas sobre privacidade.

A situação específica dos CBDCs no contexto de pagamentos envolve, conforme Jiang (Jiang, 2023), quatro principais atores: o pagador, o beneficiário, entidades processadoras como bancos centrais e comerciais, e agências de aplicação da lei, cada qual com diferentes direitos e obrigações em termos de privacidade. A abordagem da teoria da integridade contextual se destaca por adaptar a noção de privacidade aos desafios específicos enfrentados

³⁸ BCB COMUNICA. **Entenda o Projeto Piloto do Real Digital**. YouTube, 27 jul. 2023. Disponível em: https://www.youtube.com/watch?v=R42ZEyqEa_A. Acesso em: 29 ago. 2024.

por cada ator, reconhecendo que não há uma única concepção de privacidade aplicável universalmente, mas sim uma necessidade de abordagem contextualizada.

Além disso, segundo Jiang (2023) os princípios aplicáveis à transmissão de informações, que variam conforme os atores e os atributos envolvidos, desempenham um papel importante na normativa informacional dos pagamentos CBDC. Por exemplo, um pagamento pode necessitar da transmissão de dados sobre o valor monetário e as contas dos envolvidos para os processadores de pagamento, que por sua vez podem compartilhar esses dados com terceiros. Essas nuances enfatizam a complexidade dos fluxos de informação em transações CBDC e a necessidade de uma abordagem flexível para lidar com a privacidade em tais sistemas.

Avaliar quais aspectos de um pagamento CBDC devem permanecer privados envolve uma análise normativa, especialmente sobre quais informações, como dados de identidade, devem ser mantidas em sigilo do governo, público e terceiros não envolvidos na transação. Jiang (2023) sustenta que é importante reconhecer, ainda, que os pagamentos em CBDC, semelhantes aos pagamentos de varejo, deixam um rastro de dados que pode revelar detalhes íntimos da vida pessoal de um indivíduo, incluindo suas viagens e a sua situação financeira. A divulgação dessas informações a partes não relacionadas pode ameaçar significativamente a privacidade e dignidade das pessoas envolvidas.

Tensão entre a tecnologia DLT e Direito à Privacidade e ao Sigilo Bancário

Cruvinel e Prestes (2023) apontam que há uma tensão entre moedas digitais como o Real Digital (DREX) e a proteção da privacidade e do sigilo bancário em tecnologias de livro-razão distribuído (DLT). No caso brasileiro, as transações financeiras devem guardar compatibilidade com a Lei Complementar nº 105, de 2021, com a LGPD, e com os regulamentos do Banco Central do Brasil relativos à privacidade.

A natureza imutável e transparente das DLTs apresenta, segundo os autores, desafios para a proteção de dados pessoais, pois dados armazenados nesse tipo de tecnologia são geralmente considerados apenas pseudo-anonimizados. Isso significa que, com as técnicas e informações corretas, pode-se potencialmente identificar os indivíduos a partir desses dados.

Para enfrentar esses desafios, Cruvinel e Prestes (2023) apontam uma possível solução para endereçar a questão da privacidade em CBDCs - como o DREX: adotar tecnologias como protocolos de *Zero Knowledge Proof* (ZKP), ou Prova de Conhecimento Zero - um método criptográfico que permite a uma parte provar a posse de uma informação sem revelar a própria informação, utilizando princípios matemáticos e criptográficos complexos para garantir privacidade e segurança. No âmbito da Plataforma DREX, essa tecnologia permitiria, por exemplo, comprovar que uma conta possui saldo suficiente para uma transação sem expor o valor do saldo.

Entretanto, Jiang (2023) aponta que o modelo operacional de dois níveis de CBDC, como o adotado no DREX, a complexidade do fluxo de dados entre intermediários e usuários finais aumenta consideravelmente. Os intermediários - bancos centrais, bancos comerciais, instituições de pagamento - podem criar perfis detalhados dos usuários ao combinar dados do DLT do CBDC com outras informações financeiras e pessoais. Isso apresenta dois principais riscos de privacidade: o aumento de pontos de coleta de dados que ampliam a possibilidade de abuso ou uso indevido desses dados e o aumento dos riscos de segurança cibernética.

Jiang (2023) sustenta, ainda, que apesar de o sistema de dois níveis de CBDC é semelhante aos sistemas de pagamento existentes, essa visão ignora que o banco central, no modelo de dois níveis de CBDC tem acesso a um conjunto completo de dados das transações de todos os intermediários - o que eleva os riscos de potenciais problemas com vigilância, riscos de segurança cibernética e abuso de dados.

O DLT baseado em contas do DREX - sigilo bancário e privacidade

A arquitetura tecnológica escolhida pelo Banco Central do Brasil para o DREX, como mostramos, é baseada no Hyperledger Besu, com um *blockchain* (DLT) compatível com a rede Ethereum - um DLT / blockchain baseado em contas e com compatibilidade de rodar *smartcontracts*. Assim, convergente com as arquiteturas baseadas na rede Ethereum, que denomina-se “Plataforma Ethereum”, o DREX é apontado pelo Banco Central como “Plataforma DREX”.

Essas escolhas tecnológicas - compatibilidade com a rede Ethereum; funcionalidade de *smart contracts*; blockchain baseado em conta - determinam um nível menor de privacidade e sigilo desde o projeto, como mostramos anteriormente, tendo em vista que esse

tipo de DLT, embora a identidade dos participantes na rede seja anonimizada por meio de um endereço - esse endereço é único para cada participante e em múltiplas transações, o que define que as entidades que têm acesso aos dados do DLT possam fazer análise de comportamento dos endereços para identificar a pessoa física ou jurídica responsável por aquele endereço. Com isso, haveria exposição de todas as transações financeiras, hábitos de consumo, enfim, uma quebra total de sigilo bancário e de privacidade.

A escolha - em nível de projeto - desse tipo de DLT baseado em conta leva a um sistema que tem, por *design* - um nível de privacidade e sigilo menor - e que, potencialmente, o torna incompatível com a dogmática relativa ao sigilo bancário e as normas de proteção de dados e de privacidade vigentes no Brasil.

O problema de [insuficiência] de sigilo e de [insuficiência] de privacidade na Plataforma DREX fez com que o Banco Central se visse na necessidade de introduzir outras camadas de software no sistema, para tentar mitigar o fato de que a plataforma DREX, sem tais recursos, permite uma análise de comportamento de endereços, e, em última análise, permite que pessoas com acesso ao DLT do DREX, adotando mecanismos de análise de comportamento, consigam identificar as pessoas e entidades que operam cada endereço da rede.

A questão central é que as soluções testadas pelo BC para tentar solucionar o problema de falta de privacidade e de sigilo no DREX até agora não se mostraram efetivas - o que levou, inclusive, ao adiamento do lançamento de mercado do DREX, inicialmente previsto para 2024, para o final de 2025, conforme o definido no Voto 66-2024-BCB, de 15 de maio de 2024³⁹.

O item 5, i, do referido Voto 66-2024 registra que “*as soluções tecnológicas de privacidade testadas até o momento (...) **não demonstraram a maturidade necessária para que se possa garantir o atendimento de todos os requisitos jurídicos relacionados à preservação da privacidade e à proteção de dados pessoais, em conformidade com o teor da Lei no 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e da Lei Complementar no 105, de 10 de janeiro de 2001 (Lei do Sigilo Bancário)***”.

³⁹ BANCO CENTRAL DO BRASIL. Voto BCB nº 66, de 2024. Disponível em: https://normativos.bcb.gov.br/Votos/BCB/202466/Voto_do_BC_66_2024.pdf. Acesso em: 29 ago. 2024.

Privacidade no DREX: uma questão não solucionada

Em 22 de maio de 2024, o Banco Central do Brasil anunciou⁴⁰ a segunda fase do DREX, mas reconheceu que “as soluções tecnológicas de privacidade testadas até o presente estágio do Piloto não apresentaram a maturidade necessária para que se possa garantir o atendimento de todos os requisitos jurídicos relacionados à preservação da privacidade dos cidadãos, apesar de terem evoluído ao longo do tempo”.

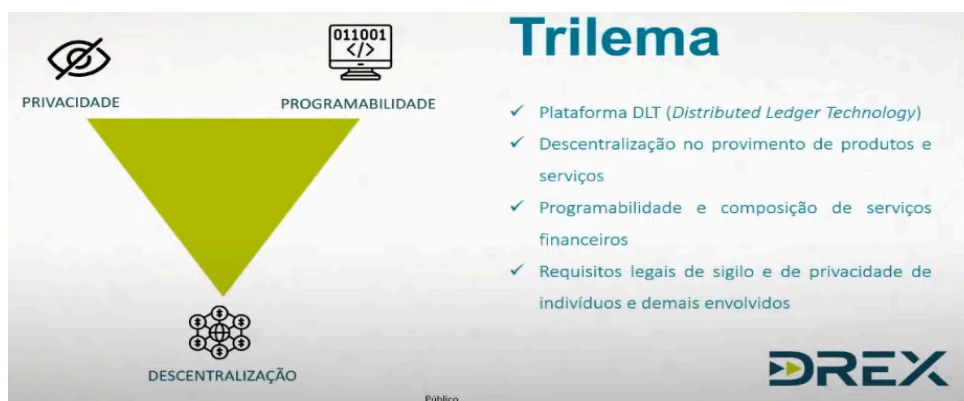


Figura 12: Trilema de privacidade no DREX - Fonte: BCB - Fórum DREX 22/05/2024⁴¹

No Fórum DREX de 22/05/2025, a coordenadora da tecnologia do DREX, Clarissa de Souza, disse que há incompatibilidade entre os três requisitos de descentralização, programabilidade e privacidade, de modo que para que se garanta, na implementação do sistema, dois desses requisitos, é necessário abrir mão de um deles.

De Souza informou que o requisito do BCB para o DREX é que a programabilidade deve ser testada de acordo com a privacidade. Além disso, estabeleceu que o Banco Central do Brasil busca uma solução de privacidade no DLT que não limite capacidade de os diversos participantes criarem serviços na rede - a questão da programabilidade do DREX. O que seria bastante diferente de buscar somente “privacidade”.

⁴⁰ BANCO CENTRAL DO BRASIL. **Nota à imprensa - Relatório de Economia Bancária de 2022**. 24 ago. 2023. Disponível em: <https://www.bcb.gov.br/detalhenoticia/18170/nota>. Acesso em: 29 ago. 2024.

⁴¹ BCB COMUNICA. **Entenda o Projeto Piloto do Real Digital**. YouTube, 27 jul. 2023. Disponível em: https://www.youtube.com/watch?v=R42ZEyqEa_A. Acesso em: 29 ago. 2024.

Durante o período inicial de testes, até maio de 2024, o Banco Central testou três soluções de privacidade: Anonymous Zetter e Starlight - estas baseadas em ZKP, e Rayls, inicialmente proposta sob o nome “Parchain”.

Situação atual relativa às questões de privacidade do DREX

Conforme apontou Clarissa De Souza em sua participação do Fórum Drex de 22/05/2024, as soluções iniciais testadas (Anonymous Zether e Starlight) mostraram certa incompatibilidade com a arquitetura de dois níveis (*w*DREX e *r*DREX).

Segundo a executiva, a solução que mostrou potencial compatibilidade de projeto com a arquitetura de Real Digital (Drex de atacado - *w*DREX) e Real Tokenizado (DREX de varejo - *r*DREX) foi a última, Rayls. Entretanto, essa potencialidade não foi ainda aferida empiricamente, nem seus potenciais problemas, tendo em vista que a fase de testes, no momento que este TCC está sendo escrito, ainda não foi iniciada.

De qualquer forma, infere-se dos relatos dos diversos executivos à frente do DREX no Banco Central do Brasil, no Fórum DREX de 22/05/2024, que os testes conduzidos com soluções baseadas em ZKP - *Zero Knowledge* - mostram dificuldades operacionais de implementar tal conceito em um sistema CBDC de dois com o Real Digital de varejo emitido pelos bancos comerciais.

DREX - privacidade e sigilo bancário

O problema de privacidade em tecnologias de tokenização e ativos digitais surge do fato de que, embora essas tecnologias permitem o armazenamento seguro de valores em um ambiente aberto, garantindo que ninguém, além do proprietário, possa alterá-los, elas também tornam essas informações visíveis para todos. Isso significa que, enquanto a propriedade e a integridade dos ativos estão protegidas, a privacidade das transações e dos saldos não está necessariamente garantida.

A transparência em *blockchains* permissionadas, como a usada pela Plataforma DREX, é restrita aos participantes da rede. No entanto, mesmo sendo restrita, a questão da privacidade é desafiadora. As informações transacionais, dados pessoais e o sigilo bancário precisam ser protegidos, mantendo-se a transparência para as partes autorizadas. A

privacidade não é apenas sobre proteger dados pessoais (conforme a LGPD), mas também sobre a confidencialidade das transações comerciais e financeiras.

No atual Sistema de Pagamentos Brasileiro, todas as transações das contas do público em geral estão sob custódia de uma entidade terceira (um "guardião"), como um banco comercial, que protege tanto a integridade quanto a privacidade das informações. Nesse ambiente, para acessar ou transferir ativos, é necessário interagir com o sistema do guardião (do banco comercial), que atua como intermediário, mas também como protetor da privacidade.

A tecnologia de tokenização muda esse paradigma e coloca os registros pseudo anonimizados em um registro distribuído e autenticado por todos os participantes. Quando os saldos e as transações de uma pessoa estão visíveis para todos, surge uma vulnerabilidade quanto ao conhecimento público de suas atividades financeiras - o que potencialmente viola o sigilo bancário - Lei Complementar nº 105, de 2001, e a Lei Geral de Proteção de Dados (LGPD).

O endereçamento desses problemas envolve adoção de camadas adicionais de privacidade, que estão ainda sendo testadas, mas encerram também um desafio técnico de integrá-las na Plataforma DREX de uma maneira que seja eficiente, não degrade a performance da rede e seja compreensível e fácil de usar pelo público em geral.

A migração para o DREX aumenta a privacidade? Diminui? Mesmo nível?

O sistema financeiro atual opera predominantemente em um modelo baseado em "silos" de informação, onde cada instituição financeira mantém suas próprias bases de dados separadamente. Dentro deste cenário, as informações são isoladas, e o acesso entre diferentes instituições é limitado. Mesmo com a introdução do *Open Finance*, que visa promover o compartilhamento de dados e a interoperabilidade entre os serviços financeiros, a realidade é que ainda existem barreiras significativas. As instituições financeiras não têm acesso amplo e direto aos dados umas das outras, mantendo a estrutura de "silos" relativamente intacta.

No entanto, com a introdução da Plataforma DREX, esse paradigma está prestes a mudar. O DREX representa uma mudança fundamental na maneira como as informações e os

dados são compartilhados e acessados dentro do sistema financeiro. Ao contrário do sistema atual, onde os dados são guardados em "silos" separados, a plataforma DREX cria um ambiente onde, a princípio, muitos dados e informações se tornam disponíveis a todos os participantes do sistema. Isso significa que as instituições que fazem parte da plataforma DREX terão a capacidade de acessar uma gama muito mais ampla de informações do que era possível anteriormente.

Este acesso expandido aos dados levanta questões significativas de privacidade e governança de dados, uma vez que requer um equilíbrio entre compartilhamento de informações e proteção dos direitos dos indivíduos. Isso significa que sem soluções adequadas de governança e tecnologia, pode haver uma visibilidade ampla e possivelmente indesejada das transações e dados dos cidadãos.

Tendo em vista os dados que coletamos na nossa pesquisa, a resposta para a pergunta do tópico é que, com a implementação do DREX a privacidade e o sigilo das transações diminuí. E caso não se adotem soluções efetivas de garantia de privacidade e de sigilo, a possibilidade de se analisar o comportamento de contas na plataforma DLT do DREX e com isso identificar a pessoa física ou jurídica a tornaria incompatível com marco regulatório vigente no Brasil relativo à privacidade e proteção de dados pessoais (LGPD), e também ao sigilo bancário - Lei Complementar nº 105, de 2001.

O DREX se amolda à dogmática do STF sobre direito de privacidade e de sigilo bancário?

No atual estágio de desenvolvimento do DREX, com base nas informações públicas divulgadas pelo Banco Central do Brasil, e pela nossa pesquisa, pode-se dizer que a Plataforma DREX **não** se amolda às diretrizes legais e constitucionais relativas ao direito de privacidade (proteção de dados pessoais) e ao sigilo bancário.

Uma parte do problema decorre das escolhas técnicas adotadas pelo Banco Central do Brasil para o DREX, sendo a definição principal de desenvolver uma CBDC dotada de compatibilidade de *smart contracts*. Essa escolha, se por um lado permite a criação de novos modelos de negócios associados com a moeda digital, por outro, envolve uma complexidade adicional e acaba direcionando as escolhas técnicas.

Isso levou a escolha do *Hyperledger Besu*, uma solução técnica para implementação de um DLT de CBDC de código aberto compatível com a EVM - Ethereum Virtual Machine, e também um modelo de DLT **baseado em contas**, diferentemente do modelo UTXO (*Unspent Transaction Output*) usado por outras criptomoedas como o Bitcoin, o que definiu desafiadoras questões de privacidade.

Especificamente em relação a opção por um DLT baseado em contas, conforme Fanti e Pocher (2022), uma desvantagem dessa arquitetura é a maior facilidade de os agentes com acesso ao DLT de vincular transações registradas a um mesmo usuário. Jiang (2023) também aponta tal problema sustentando que os dados dos usuários finais são armazenados em diversos intermediários autorizados, o que aumenta a vulnerabilidade dos dados.

Ademais, muitos intermediários, como bancos comerciais, empresas de pagamento e outras instituições financeiras, podem integrar os dados obtidos no DLT unificado do DREX com outros tipos de dados financeiros e pessoais, o que permite a tais empresas criar perfis abrangentes dos usuários. Jiang (2023) nota ainda que, ao contrário dos bancos centrais, essas entidades autorizadas a acessar o DLT têm um incentivo financeiro para monetizar os dados dos usuários.

Quanto mais completo o perfil do usuário, maior é o potencial de dano se os dados forem mal utilizados ou abusados. Além disso, esses intermediários podem compartilhar esses dados com terceiros, seja intencionalmente por razões comerciais ou involuntariamente devido a falhas de segurança, aumentando assim o risco de mau uso ou abuso dos dados. À medida que mais entidades se envolvem no manuseio dos dados, rastrear a origem de tal mau uso torna-se cada vez mais complicado.

Outro aspecto a ser considerado é as diretrizes de projeto relativas aos *smart contracts* exigem, para uma arquitetura mais robusta dos direitos de privacidade e do sigilo bancário a adoção de soluções de Prova de Conhecimento Zero (Zero-Knowledge Proof - ZKP). Entretanto, conforme comunicação do próprio Banco Central do Brasil no Fórum DREX de 22 de maio de 2024, os testes das soluções que implementam tal conceito de privacidade (ZKP) não tiveram sucesso efetivo.

Esses pontos evidenciam o desafio de alinhar essa tecnologia com a dogmática do Supremo Tribunal Federal (STF) sobre direito à privacidade e sigilo bancário - algo que até

agora o DREX **não é capaz de garantir**. Sem mecanismos eficazes para garantir a privacidade dos dados dos cidadãos e o sigilo financeiro das transações, o DREX pode enfrentar problemas jurídicos e de aceitação pelo público que está preocupado com a segurança de suas informações financeiras.

DREX - Imaginação institucional

O Drex é um exemplo de construção de mercado em que a privacidade é assegurada por design?

O BIS, em seu protótipo de CBDC de dois níveis - um design similar ao adotado no DREX - aponta que esse tipo de arquitetura de CDDC é um exemplo de implementação da privacidade dos usuários por *design* (BIS, 2022, p10).

Entretanto, o DREX não é exatamente um exemplo de construção de mercado onde a privacidade é assegurada por *design*. Embora o projeto seja de dois níveis como o protótipo do BIS, o DREX é mais ambicioso e inova ao incorporar tecnologias como o *Distributed Ledger Technology* (DLT) e *smart contracts* - o que leva a questões significativas relacionadas à privacidade que ainda precisam ser endereçadas.

A arquitetura baseada em DLT e a utilização de *smart contracts* no DREX possibilitam inovações e eficiências no sistema financeiro, mas também trazem desafios particulares em relação à privacidade dos dados. Em sistemas baseados em contas, como o utilizado pelo DREX, as transações podem - conforme Fanti e Pocher (FANTI, POCHER, 2022) - ser mais facilmente vinculadas a usuários individuais, o que potencialmente compromete o sigilo bancário e a privacidade do usuário.

Além disso, o uso de intermediários autorizados para gerenciar e armazenar esses dados pode aumentar o risco de exposição de informações sensíveis, especialmente se esses dados forem combinados com outros tipos de informações financeiras e pessoais. Embora tenham sido tentadas soluções como Provas de Conhecimento Zero (*Zero-Knowledge Proofs* - ZKP) para mitigar esses problemas, até o momento, essas soluções não se mostraram completamente eficazes ou maduras⁴².

⁴² BCB COMUNICA. **Entenda o Projeto Piloto do Real Digital**. YouTube, 27 jul. 2023. Disponível em: https://www.youtube.com/watch?v=R42ZEyqEa_A. Acesso em: 29 ago. 2024.

Portanto, ao contrário de projetos que são construídos com privacidade assegurada por *design*, onde medidas de proteção de dados são integradas no núcleo do desenvolvimento tecnológico desde o início, o DREX ainda enfrenta desafios para alcançar esse nível de segurança e proteção de dados.

O Drex elimina um conjunto de instituições que asseguram o funcionamento de um mercado com mais privacidade?

A Plataforma DREX é um empreendimento que repensa a infraestrutura e o funcionamento do sistema financeiro por meio de novas tecnologias como o *Distributed Ledger Technology (DLT)* e *smart contracts*. Esta iniciativa se alinha com as ideias de Natalino Irti e Gabriel Laender sobre a natureza artificial e construída dos mercados e a capacidade do Direito de moldar e reconstruir economicamente as instituições.

Laender, em "*O papel do Estado na construção da economia e a possibilidade do direito como imaginação institucional*" (LAENDER, 2014), demonstra que o Direito não apenas molda, mas ativamente constrói a economia, oferecendo oportunidades significativas para a criação e modificação de instituições econômicas.

Essa concepção de imaginação institucional operada pelo Direito tem um exemplo claro na atual etapa de desenvolvimento da plataforma DREX. A escolha do Banco Central por usar uma arquitetura de CBDC com funcionalidade de *smart contracts* - algo ainda não experimentado - nem mesmo nos protótipos do BIS - é um exemplo prático do conceito de imaginação institucional de Laender (LAENDER, 2014) - e que converge com o pensamento de Iurti (IURTI, 2007) sobre a natureza artificial dos mercados.

As diretrizes de *design* do DREX são exemplos de imaginação institucional com vistas a criar novos mercados e novos modelos de negócios no sistema financeiro brasileiro por meio do direito, ao estabelecer um modelo que as novas tecnologias de DLT e os *smart contracts*.

Entretanto, como ficou claro ao longo da pesquisa, a ambiciosa diretriz do Banco Central do Brasil em imaginar a reconstrução institucional do sistema financeiro brasileiro com base nessas novas tecnologias traz desafios, particularmente no que tange ao sigilo bancário e à privacidade. Esses desafios são críticos porque envolvem direitos fundamentais

constitucionalmente protegidos. O DREX, ao operar numa nova infraestrutura tecnológica, deve garantir que esses direitos sejam preservados dentro desta nova 'imaginação institucional'. O direito, neste contexto, não é apenas um conjunto de normas a serem obedecidas, mas um elemento ativo na formação da nova realidade econômica e social.

Assim, a Plataforma DREX é um exemplo contemporâneo de como o Direito, conforme discutido por Irti (IRTI, 2007) e Laender (LAENDER, 2014) molda ativamente a economia e suas instituições. Este é um momento de definição, no qual a escolha de como os novos mercados funcionarão e como influenciarão o comportamento dos agentes é fundamental para o processo de modernização proposto pelo Banco Central.

DREX - Aspectos de Regulação responsiva

Nesse contexto de implementação, a análise do *design* da Plataforma DREX sob a ótica das heurísticas da Regulação Responsiva, conforme a abordagem proposta por Aranha (ARANHA, 2023), oferece um modelo analítico no qual a regulação não se baseia primariamente em sanções punitivas, mas busca a promoção de um consenso e o estabelecimento de um diálogo construtivo entre reguladores e regulados.

A Plataforma DREX é um empreendimento que oferece ao regulador um desafio devido à complexidade de integrar múltiplos atores como bancos comerciais, instituições de pagamento e empresas de tecnologia.

Assim, a forma como o Banco Central do Brasil vem implementando o Projeto DREX, com diálogo institucional, fóruns de discussão técnica e institucional, e o fomento a soluções do mercado evidencia que o regulador atua na perspectiva de adaptação às capacidades dos regulados - uma heurística da Regulação Responsiva que sugere que os reguladores devem ajustar suas estratégias regulatórias com base nas capacidades e comportamentos dos regulados. Na arquitetura do DREX, o Banco Central promove um ambiente que busca proteger o direito ao sigilo bancário e à privacidade, mas também enfrenta um *trade-off* desses requisitos com a dinâmica de inovação tecnológica, como apontado no “Trilema de Privacidade” apontado pela Diretora de Tecnologia do Banco Central no Fórum DREX de maio de 2024.

Esse processo de debates institucionais entre o regulador e o regulado no desenvolvimento da Plataforma DREX é enquadrado também na heurística de “Fomento ao Diálogo e ao Consenso”, que, conforma Aranha (ARANHA, 2023), deve priorizar o estabelecimento de diálogos e a busca por consenso antes de recorrer a medidas punitivas. Essa questão é fundamental no processo colaborativo que envolve uma multiplicidade de *stakeholders*.

Conclusões

O Banco Central do Brasil estabeleceu uma meta ambiciosa para a CBDC brasileira, o DREX, com diretrizes que não apenas se alinham ao conceito de uma moeda digital baseada em um DLT de *blockchain*, mas também incorporam a capacidade de implementar *smart contracts*. Esta funcionalidade abre portas para o desenvolvimento de modelos de negócio inovadores, expandindo as possibilidades dentro do ecossistema financeiro.

No entanto, essa escolha ambiciosa trouxe consigo desafios significativos em termos de privacidade e proteção de dados pessoais, assim como o respeito ao sigilo bancário. Até o momento, estes desafios não foram completamente endereçados, resultando em um cenário onde o DREX não oferece o mesmo nível de proteção da privacidade e do sigilo bancário tanto para os usuários finais quanto para os operadores do sistema financeiro apresentado pelo atual Sistema de Pagamentos Braileiro.

Contudo, é importante reconhecer que o projeto ainda se encontra em uma fase de testes e desenvolvimento. Isso significa que ainda há espaço para evolução e aperfeiçoamento das soluções técnicas que podem vir a garantir a preservação da privacidade e à proteção de dados pessoais, em conformidade com a Lei no 13.709, de 14 de agosto de 2018 (LGPD), e da Lei Complementar no 105, de 10 de janeiro de 2001 (Lei do Sigilo Bancário).

Referências bibliográficas

Anuário do Observatório da LGPD da Universidade de Brasília : análise comparada entre elementos da LGPD e do GDPR / organização Laura Schertel Mendes ... [et al.]. – Brasília : Universidade de Brasília, Faculdade de Direito, 2024. 2 v. Disponível em: http://icts.unb.br/jspui/bitstream/10482/47774/1/LIVRO_AnuarioObservatorioLGPD_v2.pdf. Acesso em: 9 jul. 2024.

ABRÃO, Nelson. **Direito Bancário**. Editora Saraiva, 2019. E-book. ISBN 9788553611454. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788553611454/>. Acesso em: 14 jan. 2024.

AKCORA, Cuneyt Gurcan; GEL, Yulia R.; KANTARCIOGLU, Murat. *Blockchain networks: Data structures of Bitcoin, Monero, Zcash, Ethereum, Ripple, and Iota, 2021*. Disponível em <https://doi.org/10.1002/widm.1436>. Acesso em: 14 de jul de 2024.

ARANHA, Márcio Iorio, 1974-Manual de Direito Regulatório: Fundamentos de Direito Regulatório /Márcio Iorio Aranha. 8. ed. rev. ampl. – London : Laccademia Publishing, 2023.

STEINBERG, Daniel Fideles; ESPIR, Bárbara Cabrera. CBDCs e privacidade: notas para um debate. In: ABRUSIO, Juliana; RONCAGLIA, Ana Maria. **A LGPD explicada por especialistas em proteção de dados**. 1. ed. Belo Horizonte, São Paulo: D'Plácido, 2023. v. 1, cap. 10, p. 219-231. ISBN 978-65-5589-885-9.

BANCO CENTRAL DO BRASIL. **Real Digital: uma plataforma para as finanças “tokenizadas”**, 2023, in:Relatório de Economia Bancária (REB), 2023, Disponível em: https://www.bcb.gov.br/content/publicacoes/boxe_relatorio_de_economia_bancaria/reb2022b9p.pdf. Acesso em: 13 jul. 2024.

BCB (Brasil). O que é o DREX?: Real Digital. In: **O que é o DREX?**. [S. l.], 2023. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/drex>. Acesso em: 16 out. 2023.

BECH, Morten Linnemann; GARRATT, Rodney. *Central bank cryptocurrencies in: BIS Quarterly Review*. Setembro de 2017. Disponível em: https://www.bis.org/publ/qtrpdf/r_qt1709f.htm. Acesso em: 13 jul. 2024.

BIS. Project Aurum: A Prototype for Two-tier Central Bank Digital Currency (CBDC). In: BIS. Project Aurum: A Prototype for Two-tier Central Bank Digital Currency (CBDC). Bank for International Settlements (BIS): BIS, 2022. Disponível em: <https://www.bis.org/publ/othp57.pdf>. Acesso em: 30 maio 2024.

BLUM, Rita Peixoto F. **O Direito à Privacidade e a Proteção dos Dados do Consumidor**. Grupo Almedina, 2022. E-book. ISBN 9786556277066. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786556277066/>. Acesso em: 03 jun. 2024.

BUELAU, Alex; SANTOS, Ricardo. **Addressing Privacy Challenges in Permissioned Blockchain Adoption for Financial Institutions and Governments**. 2023. Disponível em: https://www.bcb.gov.br/conteudo/eventos/Documents/moedas_digitais/tokenizacao/WorkTOK-Mimeo-TECH_3A_C_Addresssing_Privacy_Challenges_in_Permissioned_Blockchain_Adoption_for_Fin_Instits_and_Governments.pdf. Acesso em: 3 jun. 2024.

CBDC: BIS Innovation Hub work on central bank digital currency (CBDC). [S. l.], 2023. Disponível em: <https://www.bis.org/about/bisih/topics/cbdc.htm>. Acesso em: 16 out. 2023.

CHAN, Aldar C-F. UTXO in Digital Currencies: **Account-based or Token-based? Or Both?** University of Hong Kong. Disponível em: <https://arxiv.org/abs/2109.09294v1>. Acesso em: 12 jul. 2024.

CRUVINEL, Aline; PRESTES, Jeff. **Caminhos para um Real Digital on-chain compatível com o direito à privacidade e proteção de dados pessoais desde a concepção**. 2023. Disponível em: https://www.bcb.gov.br/conteudo/eventos/Documents/moedas_digitais/tokenizacao/WorkTOK-Mimeo-TECH_3A_A_Caminhos_para_um_Real_Digital_on-chain_compativel_com_o_direito_a_privacidade_desde_a_concepcao.pdf. Acesso em: 3 jun. 2024.

DE SOUSA, Tais Maria Ferreira. **Aspectos fundamentais sobre o sigilo bancário**. In: Jus Brasil, 2020. Disponível em: <https://www.jusbrasil.com.br/artigos/aspectos-fundamentais-sobre-o-sigilo-bancario/885857633>. Acesso em: 6 dez. 2023.

Essays on Negative Interest Rates and GDP Forecasting / Fernanda Magalhães Rumenos Guardado; advisor: Tiago Couto Berriel; co-advisor: Marcelo Cunha Medeiros. – Rio de Janeiro: PUC-Rio, Departamento de Economia, 2019. Disponível em <https://www.maxwell.vrac.puc-rio.br/53509/53509.PDF>, acesso em 05/11/2023

Ethereum Virtual Machine (EVM), [s. l.], 2024. Disponível em: <https://ethereum.org/en/developers/docs/evm/>. Acesso em: 6 jun. 2024.

FANTI, Giulia; POCHER, Nadia. Privacy in Cross-border Digital Currency: A Transatlantic Approach. In: **Privacy in Cross-border Digital Currency: A Transatlantic Approach**. Frankfurt: Atlantic Council, 29 set. 2022. Disponível em: https://cris.unibo.it/retrieve/95754c60-37ef-492e-bc54-b467c6a3b155/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf. Acesso em: 6 jun. 2024.

FRANCO, Gustavo. O futuro do dinheiro. In: **O futuro do dinheiro**. Rio de Janeiro: Casa das Garças, 2020. Disponível em: <https://iepecdg.com.br/wp-content/uploads/2020/12/O-futuro-do-dinheiro-3.docx.pdf>. Acesso em: 7 jun. 2024.

FRANSISKA ARI, Fransiska Ari. CENTRAL BANK DIGITAL CURRENCY UNDER THE STATE THEORY OF MONEY:: A PRELIMINARY LEGAL ANALYSIS. **Journal of Central Banking Law and Institutions**, [s. l.], 2022. Disponível em: <https://www.jcli-bi.org/index.php/jcli/article/view/23/26>. Acesso em: 16 out. 2023.

IRTI, Natalino. **A ordem jurídica do mercado**. In: Revista de Direito Mercantil, Industrial, Econômico e Financeiro. São Paulo, n.145, p.44-49, jan / mar 2007.

ITI (Brasil). ICP Brasil. VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL. In: **VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL**. [S. l.], 2010. Disponível em:

https://mailman.iti.gov.br/images/repositorio/legislacao/documentos-principais/15/DOC-ICP-15_v.2.0.pdf. Acesso em: 9 dez. 2023.

JIANG , Jiaying. **Privacy Implications of Central Bank Digital Currency**. In: UF Law Scholarship Repository. University of Florida Levin College of Law, 2023. Disponível em: <https://scholarship.law.ufl.edu/facultypub/1222/>. Acesso em: 4 jun. 2024.

JONES, Ry. **Hyperledger Besu**. In: Hyperledger Besu. [S. l.], 2024. Disponível em: <https://wiki.hyperledger.org/display/BESU/Hyperledger+Besu>. Acesso em: 6 jun. 2024.

LAENDER, Gabriel Boavista. **O papel do Estado na construção da economia e a possibilidade do direito como imaginação institucional**. 2014. 321 f., il. Tese (Doutorado em Direito)—Universidade de Brasília, Brasília, 2014. Disponível em: <http://icts.unb.br/jspui/handle/10482/15997>. Acesso em: 2 jan. 2024.

LUZ, Andréa Oliveira S. **Sigilo Bancário: Acordos para Troca de Informações Internacionais**. [Digite o Local da Editora]: Grupo Almedina (Portugal), 2019. E-book. ISBN 9788584935185. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9788584935185/>. Acesso em: 14 jan. 2024.

MENDES, Gilmar; MARTINS, Ives Gandra da Silva. Sigilo Bancário, **Direito de Autodeterminação sobre Informações e Princípio da Proporcionalidade**. Repertório de Jurisprudência, Brasília, p. 435-438, 15 dez. 1992. Disponível em: <https://www.gilmarmendes.com.br/wp-content/uploads/2018/09/SIGILO-BANC%C3%81RIO-DIREITO-DE-AUTODETERMINA%C3%87%C3%83O-SOBRE-INFORMA%C3%87%C3%95ES-E-PRINC%C3%8DPIO-DA-PROPORCIONALIDADE.pdf>. Acesso em: 6 dez. 2023.

MEHRLING, Perry. **THE NEW LOMBARD STREET: How the Fed Became the Dealer of Last Resort**. 5. ed. United Kingdom: Princeton University Press, 2011. ISBN 78-0-691-14398-9.

Miranda, Bruno Felipe de O. **Moeda e Direito: Elementos Para uma Teoria Constitucional**. (Coleção estudos em direito público e regulatório). Disponível em: Minha Biblioteca, Grupo Almedina (Portugal), 2022.

NAKAMOTO, Satoshi. Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer. In: Bitcoin: **Um Sistema de Dinheiro Eletrônico Peer-to-Peer**. Internet, 2009. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em: 6 dez. 2023.

OLIVEIRA, Victor Augusto de Almeida. **Moeda eletrônica de Banco Central: Uma introdução**. 2019. Dissertação de Mestrado (Mestrado Economia) - USP - Universidade de São Paulo, Ribeirão Preto (SP), 2019. Disponível em: https://www.teses.usp.br/teses/disponiveis/96/96131/tde-16082019-093744/publico/VictorAAOliveira_Original.pdf. Acesso em: 16 out. 2023.

Pinto, Isabelle Carvalho Costa. O desenvolvimento da moeda digital chinesa: potencialidades e desafios para a China e o Sistema Monetário e Financeiro Internacional / Isabelle Carvalho Costa Pinto. - São Paulo, 2022. Disponível em <https://repositorio.unesp.br/server/api/core/bitstreams/470c779e-7471-4a1a-b68c-e0f1e386481d/content>, acesso em 05/11/2023

RISK, Andrew. Central Bank Digital Currency: Legal and Regulatory Issues. In: **Central Bank Digital Currency: Legal and Regulatory Issues**. [S. l.], 2022. Disponível em: <https://www.zbw.eu/econis-archiv/handle/11159/510220>. Acesso em: 16 out. 2023.

SALAMA, Bruno Meyerhof; ZELMANOVITZ, Leonidas. **Crítica à Proposta de Criação de Real Digital de "Varejo"**. In: Revista do Laboratório de Inovações Financeiras e Tecnológicas #6 Edição Especial. p238. Brasília: Fabio Araujo, 2023. Disponível em: <https://revista.liftlab.com.br/lift/issue/view/21/32>. Acesso em: 30 maio 2024.

SCHWARZ, Daniel. Central Bank Digital Currencies and competition laws: recognising the importance of competition laws in the CBDC ecosystem. In: **Central Bank Digital Currencies and competition laws: recognising the importance of competition laws in the CBDC ecosystem**. [S. l.], 2023. Disponível em: https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/03/central_bank_digital_currencies_and_competition_laws.pdf. Acesso em: 16 out. 2023.

SANTANA, José Vicente Mattos. Impacto do Novo Sistema de Pagamentos Brasileiro nos Custos dos Bancos. In: **Impacto do Novo Sistema de Pagamentos Brasileiro nos Custos dos Bancos**. [S. l.], 2005. Disponível em:

<https://www.teses.usp.br/teses/disponiveis/12/12136/tde-10022022-160519/publico/MsJoseVicenteMattosSantana.pdf>. Acesso em: 10 jul. 2024.

Fabian Schär, "**Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets**," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74. <https://doi.org/10.20955/r.103.153-74>

WANG, Heng. How to understand China's approach to central bank digital currency?. *In: How to understand China's approach to central bank digital currency?*. [S. l.], 2023. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364922001315>. Acesso em: 16 out. 2023.

ZETHER: Towards Privacy in a Smart Contract World. [S. l.], 2019. Disponível em: <https://eprint.iacr.org/2019/191.pdf>. Acesso em: 6 jun. 2024.

ZELMANOVITZ, Leonidas; SALAMA, Bruno Meyerhof. **Central Bank Digital Currency and the Agenda of Monetary Devolution**. In: BODELLINI, Marco; GIMIGLIANO, Gabriella; SINGH, Dalvinder (ed.). Commercial Banking in Transition. American Publisher Palgrave Springer, 2022. Forthcoming. Disponível em: <https://ssrn.com/abstract=4149005>. Acesso em: 09 jul. 2024.

Material audiovisual

Entrevista com Fabio Araujo - Coordenador do Drex | Real Digital: desafios e impacto na sociedade. Disponível em <https://www.youtube.com/watch?v=wX6lawVC36g&t=37s>

Transparência e privacidade no ambiente do Real Digital: Disponível em <https://www.youtube.com/watch?v=8qKs0h3eBHw>

Hyperledger Besu -- What it is and how to get involved . Disponível em https://www.youtube.com/watch?v=gF__bwiG66g

Cunha, G. (n.d.). Saindo do zero em Zero Knowledge (ZK). Blocknews. Disponível em <https://www.blocknews.com.br/opiniaao/saindo-do-zero-em-zero-knowledge-zk/>

Banco Central do Brasil. **Brazil's Real Time Gross Settlement System**. Disponível em: <https://www.bcb.gov.br/Pom/Spb/Ing/InterbankFundsTransfer/ISTR.asp?frame=1>, acesso em 13 de jul de 2024.

BANK FOR INTERNATIONAL SETTLEMENTS. Project Tourbillon explores anonymity for digital payments. Disponível em: <https://www.youtube.com/watch?v=rahFmNukBF8>. Acesso em: 13 jul. 2024.

BANCO CENTRAL DO BRASIL. Coletiva - Real Digital - 06/03/2023. Disponível em: <https://www.youtube.com/watch?v=LCycE9mfH2U>. Acesso em: 13 jul. 2024.

BANCO CENTRAL DO BRASIL. Real Digital, Workshop Piloto RD. Abril de 2024. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/workshop/Workshop_Sessao_2_ModelosDeNegocio_Piloto_RD.pdf. Acesso em: 13 jul. 2024.

AN INTRODUCTION TO HYPERLEDGER. Disponível em: https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/Hyperledger/Offers/HL_Whitepaper_IntroductiontoHyperledger.pdf. Acesso em: 13 jul. 2024.

BANCO CENTRAL DO BRASIL. Fórum Drex. [S.l.], 22 abr. 2024. Disponível em: https://www.youtube.com/watch?v=R42ZEyqEa_A. Acesso em: 13 jul. 2024.

BOMFIM, Ricardo. O que é a Hyperledger Besu? Conheça o blockchain que será usado para o real digital. Valor, 06 mar. 2023. Disponível em: <https://valor.globo.com/financas/criptomoedas/noticia/2023/03/06/o-que-e-o-hyperledger-besu-conheca-o-blockchain-que-sera-usado-para-o-real-digital.ghtml>. Acesso em: 13 jul. 2024.

STEIL, Juliana. DREX e privacidade: Veja três soluções contra exposição de dados. Valor Econômico, 07 dez. 2023. Disponível em: <https://valor.globo.com/financas/criptomoedas/noticia/2023/12/07/drex-e-privacidade-veja-as-tres-solucoes-contras-exposicao-de-dados.ghtml>. Acesso em: 13 jul. 2024.

STEIL, Juliana. O que é a Hyperledger Besu e por que o BC a escolheu para o DREX. Valor Econômico, 07 dez. 2023. Disponível em:

<https://valor.globo.com/financas/criptomoedas/noticia/2023/12/07/o-que-e-a-hyperledger-besu-e-por-que-o-bc-a-escolheu-para-o-drex.ghtml>. Acesso em: 13 jul. 2024.

STEIL, Juliana. O que é o DREX? É muito mais que uma moeda digital. Valor Econômico, 07 dez. 2023. Disponível em: <https://valor.globo.com/financas/criptomoedas/noticia/2023/12/07/o-que-e-o-drex-e-muito-mais-que-uma-moeda-digital.ghtml>. Acesso em: 13 jul. 2024.