CADERNOS IFD

Infraestruturas de mercado financeiro e DLT/Blockchain

Volume 5

Tecnologias de Registro Distribuído (DLT) e IMFs

Instituto de Finanças Digitais (IFD)

2026

Cadernos IFD — Infraestruturas de mercado financeiro e DLT/Blockchain

Volume 5 — Tecnologias de Registro Distribuído (DLT) e IMFs

Instituto de Finanças Digitais (IFD)

2026

Coordenador Geral: Ricardo Paixão

Coordenadores Técnicos: Isac Costa, Maria Julia Person Argollo e Rodrigo de Abreu Pinto

Pesquisadores: Eduarda Caldas, Gabriel Barenco, Geovana Soares, Guilherme Melchior, João Felipe Bezerra Assis, Jorge Aragão, Lucas Caminha, Marcelo Vaz de Oliveira Júnior, Pedro de Menezes Carvalho, Tarcísio de Souza Neto, Tarik Machado

Sobre o IFD

O Instituto de Finanças Digitais (IFD) é pessoa jurídica de direito privado, sem fins lucrativos, qualificada como Instituição de Ciência, Tecnologia e Inovação (ICT) nos termos da Lei nº 10.973/2004. Sua missão institucional consiste em formar pesquisadores e desenvolver estudos voltados ao avanço tecnológico do mercado financeiro e de capitais brasileiro.

No âmbito do Acordo de Cooperação Técnica celebrado com a Comissão de Valores Mobiliários (CVM) em outubro de 2023, o IFD coordena pesquisas e estudos sobre o arcabouço regulatório do mercado de capitais, com o propósito de contribuir para o fomento da inovação tecnológica e de oferecer subsídios técnicos ao regulador em eventuais processos de atualização normativa.

As atividades de pesquisa que deram origem a esta série contam com o apoio da Fundação de Apoio à Pesquisa do Distrito Federal (FAP-DF), responsável pela concessão de bolsas a jovens pesquisadores.

Apresentação da série

A série *Cadernos IFD — Infraestruturas de mercado financeiro e DLT/Blockchain* reúne, em volumes independentes, os resultados da pesquisa conduzida pelo Instituto de Finanças Digitais (IFD) no âmbito do Acordo de Cooperação Técnica firmado com a Comissão de Valores Mobiliários (CVM) em outubro de 2023.

A pesquisa examinou, de forma exploratória e sistemática, a interação entre o uso de tecnologias de registro distribuído (*Distributed Ledger Technology*, DLT) e o arcabouço normativo aplicável aos prestadores de serviços do mercado de capitais brasileiro, com atenção às implicações regulatórias decorrentes da adoção dessas tecnologias. O trabalho articulou o exame dos fundamentos tecnológicos da DLT, o mapeamento das normas vigentes aplicáveis às infraestruturas de mercado financeiro e aos serviços correlatos, a avaliação das práticas dos participantes do mercado brasileiro, o estudo de experiências internacionais e a análise de recomendações de organismos multilaterais.

O objetivo central foi identificar em que medida o regime regulatório vigente acomoda o uso de DLT por prestadores de serviços do mercado de capitais e onde eventuais ajustes normativos se mostram necessários, de modo a preservar a integridade das transações, a proteção dos investidores e o funcionamento adequado das infraestruturas de mercado.

O relatório final, organizado em onze capítulos, é publicado nesta série como nove cadernos independentes. Os oito primeiros capítulos correspondem a um caderno cada. Os três capítulos finais, dedicados às oportunidades e aos riscos, às propostas de adaptação normativa e às conclusões, reúnem-se em um caderno consolidado, o mais substantivo da série:

1. Introdução
2. Infraestruturas de Mercado Financeiro: Funções e Regulação

3. Regulação da CVM sobre IMFs e serviços correlatos
4. Mercados organizados e intermediação
5. Tecnologias de Registro Distribuído (DLT) e IMFs
6. Visão dos prestadores de serviços no Brasil
7. Experiências internacionais
8. Diretrizes de organismos multilaterais
9. Mapeamento de Riscos e Oportunidades para a Regulação

Cada caderno reproduz na íntegra o conteúdo correspondente do relatório. As adaptações limitam-se a ajustes editoriais destinados à leitura autônoma do volume, ao realinhamento da numeração das seções e das notas de rodapé e ao acréscimo de elementos visuais derivados do próprio texto.

Este caderno corresponde ao Capítulo 5 do relatório e trata de como a tecnologia de registro distribuído afeta custódia, liquidação, gestão de garantias e interoperabilidade, e das arquiteturas possíveis para as infraestruturas de mercado.

Sumário

Tópicos deste caderno

Este caderno examina o uso de Tecnologias de Registro Distribuído (*Distributed Ledger Technology*, DLT) nas infraestruturas do mercado financeiro (IMFs) e o modo como a tokenização de valores mobiliários redistribui funções entre os atores da cadeia de pós-negociação. O ponto de partida é a pergunta sobre a existência de um problema efetivo a ser resolvido, seguida do exame das decisões de arquitetura tecnológica, dos tipos de rede e dos mecanismos de consenso, e de suas consequências jurídicas para a propriedade fiduciária, a constituição de gravames e a execução de garantias.

A análise percorre as atividades reguladas afetadas pela tecnologia, entre elas a custódia e o depósito centralizado, a liquidação e a finalidade (*settlement finality*), a gestão de garantias, a proteção patrimonial por segregação e seguros, além dos dados, da interoperabilidade e do cadastro. Discute os riscos operacionais, cibernéticos e de governança, o trilema da DLT e os impedimentos ao desenvolvimento de mercado. Encerra com as arquiteturas possíveis, do reposicionamento dos intermediários à proposta de depositário digital e aos modelos unificadores, e confronta as infraestruturas baseadas em DLT com os Princípios para Infraestruturas do Mercado Financeiro (PFMI).

1. Ponto de partida: existe mesmo um problema a ser resolvido?

A discussão sobre o uso de DLT nas infraestruturas do mercado financeiro costuma ser apresentada como resposta tecnológica a problemas autoevidentes. Antes de avaliar arquiteturas ou modelos de tokenização, porém, é preciso enfrentar a pergunta enunciada no título desta seção.

Em outros termos, *o desenho atual das IMFs apresenta ineficiências que justifiquem uma reengenharia tecnológica de fundo, ou as fricções observadas são custos inerentes às funções que essas infraestruturas exercem*? Sem esse exame prévio, corre-se o risco de tratar a DLT como solução em busca de problema, uma objeção mais abrangente e recorrente em torno da tecnologia aqui discutida[1].

Alguns elementos da resposta a estas questões já foram abordados em seções anteriores.

Por exemplo, o ciclo de liquidação T+2, ainda predominante em mercados de ações no Brasil, mantém um intervalo entre negociação e liquidação que gera exposição de contraparte, imobilização de garantias e custo de capital regulatório. Esse intervalo não decorre de limitações tecnológicas dos sistemas centrais, que operam em ciclos mais curtos, mas da necessidade de coordenação entre múltiplas infraestruturas, intermediários e agentes de

[1] A premissa de que a blockchain e as Tecnologias de Registro Distribuído (DLT) podem ser uma "solução em busca de um problema" é amplamente debatida na literatura, sendo a tecnologia frequentemente descrita como "superestimada" ou metaforicamente apontada como "um martelo à procura de um prego" no contexto das Infraestruturas de Mercado Financeiro (IMF). LOADER, David. *Clearing, Settlement and Custody*. 3. ed. Oxford: Butterworth-Heinemann, 2020. Ainda, sobre a complexidade e polarização do debate: "Sitting at the cross-section of financial services, technology and changing demographics, it is one of the most widely discussed but perhaps often misunderstood subjects in the industry". JIANG. Crossing the chasm: Why post-trade FMIs are the key to scaling blockchain adoption. *Journal of Securities Operations & Custody*, v. 17, i. 2, pp. 119-129, fev. 2025. A viabilidade do uso de DLTs no ambiente de pós-negociação é problematizada devido a uma série de "abismos" (*chasms*) que dificultam a sua adoção em larga escala. Estes obstáculos incluem a falta de casos de negócios claros e viáveis que justifiquem o investimento, altos custos de implementação e transição de sistemas, bem como desafios significativos de segurança, escalabilidade e interoperabilidade.

custódia, cada qual com seus próprios processos de confirmação, alocação, conciliação e instrução.

A coordenação se sustenta sobre a reconciliação de bases de dados fragmentadas, mantidas por participantes distintos da cadeia de pós-negociação. Cada base é, por construção, um registro soberano dentro do seu domínio funcional, e a integridade do conjunto depende da correspondência permanente entre elas. Essa correspondência é assegurada por conciliação diária em vários níveis, o que é eficaz, mas oneroso.

A isso se soma uma sobreposição funcional parcial entre infraestruturas e prestadores de serviço. O mesmo evento, seja uma transferência de titularidade, o pagamento de um provento ou a constituição de um gravame, pode ser refletido em múltiplos sistemas, cada qual com lógica operacional, requisitos de mensageria e janelas de processamento próprios.

A interoperabilidade entre essas camadas exige investimento contínuo em integração, governança de dados e tratamento de exceções. O resultado é uma estrutura de custos que se concentra em atores de maior escala e constitui barreira à entrada de emissores menores e novos participantes.

Esse diagnóstico, contudo, não conduz à conclusão de que tecnologia é suficiente para lidar com gargalos e ineficiências atuais das IMFs. As infraestruturas centrais institucionalizam confiança, internalizam riscos sistêmicos, organizam respostas coordenadas a cenários de inadimplemento e operam como ponto de articulação entre regulação prudencial, política monetária e disciplina de mercado.

As cascatas de salvaguardas das contrapartes centrais, a titularidade fiduciária dos depositários, os mecanismos de gestão de inadimplementos e a integração com sistemas de pagamento em escala são a razão pela qual essas infraestruturas são objeto de regulação intensa e supervisão coordenada entre autoridades.

Um protocolo, por mais sofisticado, não substitui uma deliberação em situação de crise, não absorve perdas de inadimplemento, não responde a determinações judiciais sobre bloqueios e não exerce função autorregulatória sobre seus participantes. Em essência, é uma ferramenta que pode ser útil e aumentar a eficiência do sistema[2], mas não é suficiente em si mesma para endereçar os problemas e alcançar os objetivos pretendidos na dinâmica das IMF – assim como um *smart contract* é apenas um recorte operacional de um contrato no sentido jurídico do termo.

A pergunta mais adequada, portanto, seria como o uso de DLT reorganizar parte de suas funções de modo a reduzir custos de coordenação, encurtar ciclos, melhorar interoperabilidade e ampliar o acesso, sem comprometer as funções institucionais que as justificam.

Essa reformulação desloca o debate da desintermediação para o redesenho de infraestrutura sob novos parâmetros tecnológicos. Avaliar essa hipótese exige enfrentar as escolhas arquiteturais subjacentes a qualquer utilização de DLT em infraestruturas reguladas.

1.1.Decisões de arquitetura

A primeira decisão em termos de arquitetura tecnológica diz respeito à camada em que a infraestrutura se constitui. Soluções de primeira camada implicam construir uma rede própria, com regras de consenso e governança desenhadas para o mercado de capitais. Soluções de segunda camada operam sobre redes preexistentes, herdando suas propriedades de segurança, mas dependendo de mecanismos de comunicação e ancoragem com a camada base.

[2] Mesmo o discurso de maior eficiência costuma ser colocado em xeque. Plataformas de liquidação convencionais (como o sistema TARGET2-Securities europeu) já entregam liquidação atômica e entrega contra pagamento (DvP) em níveis de eficiência que expõem as fragilidades das DLTs, as quais muitas vezes ainda sofrem com altos custos de rede e estruturas de governança opacas. Cf. MILKAU, U. Will tokenisation deliver efficiency? And what kind? *Journal of Securities Operations & Custody*, v. 17, n. 1, p. 79-94, dez. 2024.

A escolha envolve *trade-offs* entre soberania operacional, custo de manutenção, segurança herdada e capacidade de evolução do protocolo[3].

A segunda escolha refere-se ao tipo de rede. Redes públicas oferecem transparência e neutralidade operacional, mas levantam questões de finalidade jurídica, governança difusa e conformidade regulatória[4]. Redes permissionadas viabilizam controle de acesso e identificação dos validadores, ao custo de reproduzirem, em alguma medida, a centralidade institucional que a tecnologia distribuída prometeria atenuar. Modelos híbridos tentam combinar essas propriedades, com camadas permissionadas para emissão e custódia e camadas abertas para negociação.

---

[3] A decisão arquitetural de utilizar soluções de primeira camada (Layer 1) ou de segunda camada (Layer 2) em infraestruturas de mercado financeiro reflete um debate sobre onde a lógica de negócios e o processamento de transações devem ser executados. Feenan et al. (2020) discutem essa escolha utilizando a situação hipotética de automação de fluxos de caixa e execução de garantias (colaterais) em caso de inadimplência via contratos inteligentes: se a arquitetura for de Layer 1, toda a lógica de negócios residirá e será processada na própria blockchain; caso a opção seja por Layer 2, a blockchain principal atuará majoritariamente como uma plataforma de liquidação e garantia de execução correta, enquanto o processamento das regras ocorrerá fora da cadeia principal. Cf. FEENAN, Sara et al. Decentralized Financial Market Infrastructures: Evolution from Intermediated Structures to Decentralized Structures for Financial Agreements. *Journal of FinTech*, v. 1, n. 1, 2021. Em complemento, Colle explica que os protocolos de segunda camada funcionam como sistemas de compensação (*netting*) paralelos, de forma semelhante às câmaras de compensação (*clearinghouses*) tradicionais. Na prática, as transações ocorrem em ambiente *off-chain* para reduzir a sobrecarga, sendo aglutinadas e condensadas em grupos antes de serem liquidadas e ancoradas definitivamente na primeira camada. Como exemplos dessa arquitetura de segunda camada, o autor menciona a Lightning Network (utilizada para escalar a rede Bitcoin) e a solução Optimism (aplicada na rede Ethereum). Cf. COLLE, L. Reaching for the Moon: An Analysis of Real-Time Securities Clearing and Settlement in Light of Emerging Blockchain Technologies. *Virginia Law & Business Review*, v. 16, n. 3, p. 601-646, 2022.

[4] De forma sucinta, elas podem ser definidas como: (i) Públicas/Não permissionadas: Permitem acesso irrestrito para qualquer pessoa visualizar o livro-razão (*ledger*), enviar transações e atuar como um nó no processo de validação de novos blocos, sem a necessidade de uma autorização central; (ii) Privadas: Restringem o acesso de leitura e visualização dos dados a uma lista designada de usuários aprovados, e as transações geralmente ocorrem apenas por meio de interfaces oferecidas pelo operador da rede; Permissionadas: Limitam a capacidade de validar transações e adicionar blocos à rede a um conjunto restrito e conhecido de entidades previamente autorizadas. Cf. WORLD BANK. *Distributed Ledger Technology and Secured Transactions Frameworks*: A Primer. Washington, DC, 2020 (Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series, Note 3).

A terceira escolha envolve o mecanismo de consenso, que condiciona diretamente a finalidade da liquidação. Mecanismos baseados em prova de trabalho (PoW) ou prova de participação (PoS) oferecem finalidade probabilística, incompatível com o requisito de finalidade da liquidação (*settlement finality*) do Princípio 8 dos PFMI [5]. Mecanismos de tolerância bizantina a falhas (como pBFT) em redes permissionadas oferecem finalidade determinística no momento do consenso, propriedade que se aproxima do regime exigido pelas IMFs reguladas[6]. A escolha do mecanismo determina se a infraestrutura pode ser tratada como ambiente de liquidação definitiva.

No que concerne à segunda e terceira escolhas mencionadas nos parágrafos anteriores, o critério de decisão arquitetural para IMFs tipicamente recai sobre o equilíbrio entre segurança cibernética descentralizada e a necessidade de escalabilidade, privacidade e conformidade regulatória[7].

---

[5] Nesses casos, embora a probabilidade de reversão da transação diminua à medida que novos blocos são adicionados, o assentamento técnico nunca atinge a certeza absoluta, deixando o sistema vulnerável a bifurcações (*forks*) e desalinhado com a exigência dos PFMI de prover liquidação final, clara e juridicamente irrevogável. Cf. BANK FOR INTERNATIONAL SETTLEMENTS (BIS); INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*. Basileia: BIS/IOSCO, 2022. Disponível em https://www.bis.org/cpmi/publ/d206.htm. Todos os *links* deste documento foram acessados em 28 de julho de 2026.

[6] O algoritmo de consenso de Tolerância Prática a Falhas Bizantinas (pBFT) centraliza a submissão de novos dados em um nó líder predeterminado, exigindo um quórum de confirmações dos demais participantes para a atualização do livro-razão. Embora enfrente desafios de escalabilidade devido ao aumento exponencial de mensagens à medida que a rede cresce e exija a prévia validação e identificação dos nós líderes, o pBFT destaca-se por viabilizar acordos rápidos e definitivos com baixo consumo de recursos e pegada de carbono muito reduzida. WORLD BANK. *Distributed Ledger Technology and Secured Transactions Frameworks*: A Primer. Washington, DC, 2020 (Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series, Note 3).

[7] COMMITTEE ON CAPITAL MARKETS REGULATION (CCMR). *Blockchain and securities clearing and settlement*. Cambridge, MA, 2019. Disponível em: https://capmktsreg.org/wp-content/uploads/2022/11/CCMR_statement_Blockchain_Securities_Settlement-Final-1.pdf. O Committee on Capital Markets Regulation (CCMR) é um *think tank* independente e não partidário dedicado a pesquisa sobre regulação dos mercados de capitais dos EUA, com foco em eficiência dos mercados e estabilidade do sistema financeiro. O comitê é formado por algumas dezenas de líderes do setor financeiro (bancos, corretoras, gestoras de recursos, fundos privados, seguradoras), além de acadêmicos e ex-*policymakers*.

Blockchains públicas priorizam a descentralização extrema, mas para evitar ataques de usuários anônimos exigem mecanismos de consenso computacionalmente dispendiosos e lentos (como o *Proof-of-Work*), sacrificando fortemente a capacidade de processamento de transações em massa.

Por esse motivo, o arranjo usualmente sugerido para IMF é o de blockchains privadas e permissionadas[8]. Os critérios que direcionam a essa escolha são: (i) a possibilidade de identificar e responsabilizar os participantes (essencial para regras de PLD/FTP); (ii) garantir diferentes níveis de privacidade nas informações das negociações para proteger estratégias dos investidores; e (iii) permitir o uso de algoritmos de consenso muito mais rápidos e eficientes, uma vez que todos os nós validadores são entidades supervisionadas e confiáveis.

A quarta escolha trata dos incentivos econômicos dos participantes da rede. Em redes públicas, esses incentivos são embutidos no protocolo. Em redes permissionadas voltadas ao mercado de capitais, o desenho de incentivos precisa ser conciliado com a governança institucional, incluindo regras de remuneração, responsabilização por falhas e tratamento de conflitos de interesse[9].

---

[8] BERWANGER, Antonio Carlos. *Tokenização de valores mobiliários: a digitalização em redes de blockchain como alternativa à emissão e à cadeia de pós-negociação tradicional em mercados organizados de valores mobiliários*. 2025. Dissertação (Mestrado em Direito da Regulação) – Fundação Getulio Vargas, Escola de Direito do Rio de Janeiro, Rio de Janeiro, 2025 (ver Capítulo 4 – Características essenciais das redes DLT e Seção 5.2.2.1: Tipos de redes blockchain e sua compatibilização com as recomendações e princípios internacionais).

[9] Em uma perspectiva de arquitetura de mercado, a implementação de infraestruturas financeiras descentralizadas (dFMI) propõe um realinhamento de incentivos em que os riscos e as responsabilidades passam a ser assumidos proporcionalmente pelos participantes que os geram. Nessa estrutura, o capital mutualizado permanece atrelado às decisões dos investidores, substituindo a lógica tradicional de socialização de perdas típica das Contrapartes Centrais (CCPs) por uma responsabilização direta baseada no risco. Contudo, a teoria econômica alerta que serviços essenciais como a gestão de risco comportam-se como bens privados ou de clube, gerando fortes incentivos mercadológicos para que sua oferta permaneça centralizada, o que questiona se a tecnologia DLT isoladamente teria força para alterar a estrutura de incentivos e promover a desintermediação total das CCPs. Cf. PLATA, Rafael et al. Decentralised clearing?

A quinta escolha envolve o ativo de liquidação. Se a infraestrutura registra titularidade tokenizada, mas depende de liquidação financeira em sistema externo, mantém-se o descasamento entre as duas pernas da operação. A integração com stablecoins, depósitos tokenizados ou moedas digitais de banco central altera essa equação e será analisada adiante[10].

A sexta escolha refere-se à interoperabilidade entre redes. Pontes entre redes heterogêneas acumulam, na experiência internacional, histórico relevante de incidentes de segurança[11]. Em um ambiente regulado, a confiabilidade dessas pontes precisaria ser equiparável à dos mecanismos atuais de interconexão entre infraestruturas, o que exige soluções técnicas e desenho jurídico capaz de atribuir responsabilidades em cenários de falha.

A sétima escolha envolve o uso de contratos inteligentes para automação de fluxos. Contratos inteligentes permitem codificar regras operacionais de modo a executá-las automaticamente quando satisfeitas as condições. Esse

---

An assessment of the impact of DLTs on CCPs. *Journal of Securities Operations & Custody*, vol. 16(3), pages 227-246, jun. 2024.

[10] OECD. *Tokenisation of assets and distributed ledger technologies*. Paris, 2025. Disponível em https://www.oecd.org/en/publications/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_40e7f217-en.html. O relatório discute, entre outros pontos, a necessidade de utilizar CBDCs, depósitos tokenizados ou stablecoins reguladas para o "*cash leg*" de operações tokenizadas, inclusive em arranjos híbridos *on-chain*/*off-chain* em infraestruturas de mercado. Ver também: BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *Tokenisation in the context of money and other assets*: concepts and questions. Basel, 2023. Disponível em https://www.bis.org/cpmi/publ/d225.pdf. O documento examina o uso de diferentes formas de "tokenised money" (incluindo stablecoins, deposit tokens e CBDCs) para liquidação em DLT, destacando modelos em que a liquidação de ativos ocorre *on-chain* enquanto o pagamento pode ser feito *off-chain* ou com vários tipos de tokens de dinheiro emitidos por entidades reguladas. Os autores analisam como stablecoins, depósitos tokenizados e CBDCs podem ser integrados em arranjos de liquidação baseados em blockchain para reduzir risco de liquidação, permitir DvP programável e combinar trilhas *on-chain* com trilhas de pagamento *off-chain* operadas por intermediários regulados.

[11] LI, Ningran; QI, Minfeng; XU, Zhiyu; ZHU, Xiaogang; ZHOU, Wei; WEN, Sheng; XIANG, Yang. Blockchain cross-chain bridge security: challenges, solutions, and future outlook. *Distributed Ledger Technologies: Research and Practice*,, v. 4, n. 1, art. 8, p. 1-34, 2025. Disponível em: https://doi.org/10.1145/3696429; CHEN, Shengnan. A security analysis of Web3.0 cross-chain bridges. In: *CAICE '25: Proceedings of the 4th International Conference on Computer, Artificial Intelligence and Control Engineering*, 4. ACM, 2025. Disponível em: https://doi.org/10.1145/3727648.3727685.

ganho de eficiência convive com riscos próprios, como erros no código, ambiguidade na tradução de obrigações jurídicas para lógica computacional e dificuldade de adaptação a decisões judiciais supervenientes. Em infraestruturas reguladas, a automação precisa coexistir com mecanismos de *override* controlado e auditoria contínua[12].

A oitava escolha envolve as salvaguardas de segurança cibernética. As exigências regulatórias vigentes precisam ser reinterpretadas para o ambiente distribuído, em que a superfície de ataque inclui chaves criptográficas, nós validadores, oráculos e contratos inteligentes. A perda ou o comprometimento de chaves introduz uma categoria de risco sem paralelo direto na infraestrutura tradicional.

1.2.Consequências jurídicas

As escolhas de arquitetura tecnológica são instrumentais para a questão de fundo, que é saber como a DLT pode operacionalizar regras como a propriedade fiduciária do depositário central, a constituição de ônus e gravames, a verificação da existência e titularidade dos ativos, o tratamento de eventos corporativos e a execução de garantias[13].

---

[12] YAO, Qian. Blockchain-based New Financial Infrastructures: Theory, Practice and Regulation. Singapore: Spinger, 2022 (ver seção 8.4.3 Security of Smart Contracts). O conceito de *override* de *smart contracts* está associado à criação de um mecanismo de intervenção que permita a suspensão ou a terminação da execução do código em cenários específicos. Como os *smart contracts* possuem uma certeza inerente e carecem da flexibilidade e da opcionalidade presentes nos contratos tradicionais, essa capacidade de intervenção atua como uma salvaguarda essencial de governança e gestão. No âmbito da supervisão regulatória, esse mecanismo possibilita que os reguladores possam bloquear a inserção de *smart contracts* que não estejam em conformidade na blockchain, revogar o direito dos usuários de executarem esses códigos e, até mesmo, ajustar ou intervir nos parâmetros do *smart contract*.

[13] FACKLMANN, Juliana; SEVILHA, Paloma Alvares; DURAN, Camila Villard. Infraestruturas de mercado financeiro em registro distribuído: uma abordagem institucional das atividades de depositário central e de sistemas de liquidação. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, São Paulo, ano LIX, n. 180/181, p. 15-62, 2024. Disponível em: https://revistas.usp.br/rdm/article/view/217012. As autoras analisam a aplicação de DLT nas atividades de depositários centrais, ressaltando que a tecnologia viabiliza o controle preciso da titularidade e a conciliação de posições, enquanto a execução de garantias e a imposição de

A propriedade fiduciária supõe a transferência da titularidade do valor mobiliário ao depositário, com segregação patrimonial em contas individualizadas. A tradução desse arranjo para um ambiente tokenizado exige que a representação digital do ativo carregue, de forma juridicamente vinculante, a relação fiduciária subjacente. A simples emissão de um token não cria propriedade fiduciária, ao menos no contexto atuação da regulação sobre o tema no Brasil. Assim, é necessário pensar em um desenho institucional que conecte representação tecnológica e regime jurídico.

A constituição de ônus e gravames pode ser implementada por marcações em contas tokenizadas ou por contratos inteligentes que condicionem a transferência à inexistência de bloqueios. O ganho potencial é a redução do risco de divergência entre o registro do gravame e a circulação do ativo, hoje mitigada pela conciliação diária. A condição é que a marcação tenha eficácia jurídica equivalente à do registro tradicional e que a infraestrutura possa responder a determinações emitidas por autoridades competentes.

A verificação da existência e titularidade dos ativos é, em ambientes tokenizados, facilitada pela possibilidade de conferência direta dos saldos por qualquer participante autorizado. Ao mesmo tempo, quando o token representa um ativo externo à rede, a correspondência entre ambos depende de mecanismos de oráculo, custódia do ativo de referência e prova periódica de

---

gravames podem ser operacionalizadas de forma eficiente por *smart contracts* e *swaps* atômicos, o que requer adequações regulatórias para garantir segurança jurídica. Além disso: WORLD BANK. *Distributed Ledger Technology and Secured Transactions Frameworks*: A Primer. Washington, DC, 2020. O documento explora como a tecnologia de registro distribuído pode ser implementada em registros de garantias (*collateral registries*) para dar publicidade e registrar direitos de propriedade, destacando que scripts distribuídos e *smart contracts* possibilitam uma automação sem precedentes na formação, na performance e no *enforcement* de acordos de garantia e liquidação de colaterais. E ainda: MEIJER, Carlo R. W. de. The roles of CSDs in a blockchain environment. *Journal of Securities Operations & Custody*, v. 12, n. 2, p. 167-174, 2020. O autor destaca que, em um ecossistema DLT, os depositários centrais (CSDs) mantêm sua função notarial para a verificação da existência e registro inicial dos ativos, enquanto a tecnologia atua no registro imutável da transferência de titularidade e permite o uso de contratos inteligentes para automatizar ações corporativas e o penhor de valores mobiliários (*pledging of shares)*.

lastro. Em emissões nativamente digitais, o problema se atenua. Em emissões que representam ativos do mundo físico, permanece central.

A automação de eventos corporativos, como pagamento de dividendos, juros, amortizações e exercício de direitos, é uma das aplicações com maior potencial de simplificação. Contratos inteligentes podem executar esses fluxos diretamente sobre as posições tokenizadas. A condição é que o fluxo financeiro correspondente esteja disponível na mesma rede ou que existam mecanismos confiáveis de articulação com sistemas externos.

A execução de garantias e as cascatas de salvaguardas das contrapartes centrais constituem o teste mais exigente. A liquidação atômica de garantias é tecnicamente viável em ambiente tokenizado, mas a lógica de mutualização de perdas e recomposição de fundos envolve julgamento institucional e coordenação com autoridades. A DLT pode reduzir custos operacionais em fluxos rotineiros, mas a função institucional da CCP em situações de estresse permanece deliberativa e regulada.

A conclusão preliminar é que existe um problema a ser endereçado, mas sua natureza é mais limitada do que sugere o discurso de ruptura ou disrupção. Há ineficiências de coordenação, custos de reconciliação e barreiras de acesso que constituem objeto legítimo de reforma. Contudo, há, ao mesmo tempo, funções institucionais que não são redutíveis a protocolo.

A pergunta regulatória relevante que exploraremos nas seções a seguir é: *como aproveitar os ganhos potenciais da DLT preservando as funções institucionais que justificam a existência das IMFs*.

A análise das funcionalidades em que a DLT pode operar nas infraestruturas de mercado exige um detalhamento no nível das atividades reguladas. Os domínios em que o impacto regulatório tende a ser mais imediato são a custódia, depósito e a liquidação. Eles concentram o controle das posições e a execução definitiva das obrigações, e é em torno deles que se organizam, no debate internacional, as principais propostas de adaptação normativa.

A custódia e o depósito centralizado são atividades distintas, cada uma disciplinada por resolução própria e com funções institucionais que, embora complementares, não se confundem. O custodiante representa o investidor perante a infraestrutura, mantém contas individualizadas e processa instruções de movimentação. O depositário central exerce controle centralizado da titularidade fiduciária, disciplina a circulação do ativo e integra a cadeia de pós-negociação com os sistemas de compensação e liquidação. A distinção é relevante do ponto de vista regulatório.

Este capítulo, contudo, aborda as duas atividades em seção conjunta. A opção metodológica se justifica por três razões.

A primeira decorre do objeto técnico sob análise. Em ambientes tokenizados, tanto a custódia quanto o depósito centralizado operam sobre o mesmo objeto primário, que é a chave criptográfica com capacidade de movimentar o token. Quem detém a chave controla o ativo. Essa propriedade reduz, no plano operacional, parte da separação funcional que sustenta a distinção regulatória tradicional. Tratar as duas atividades em conjunto permite examinar, de forma integrada, os problemas de guarda, autorização, segregação e reconciliação que a tecnologia comum lhes impõe.

A segunda razão é que as propostas internacionais de adaptação normativa para ambientes tokenizados tendem, elas próprias, a tratar as duas atividades de forma articulada. Modelos como o Unified Ledger, as Redes de Responsabilidade Regulada e os regimes de DLT Pilot assumem, em graus variados, que a guarda e o controle centralizado da titularidade podem ser exercidos sobre a mesma infraestrutura, com redistribuição de funções entre participantes. A análise agrupada acompanha o enquadramento que o debate regulatório comparado vem adotando.

A terceira razão é de economia analítica. O exame separado reproduziria, em grande medida, as mesmas discussões sobre modelos de guarda de chaves, segregação *on-chain* e *off-chain*, validação de transações e reconciliação. A

consolidação permite tratamento mais denso, evitando repetição de argumentos que se aplicam indistintamente às duas atividades.

Essa opção metodológica não implica fusão funcional das duas atividades no plano regulatório. A seção 4, ao analisar o reposicionamento dos intermediários tradicionais, retoma a distinção entre custódia de ativos virtuais, custódia de valores mobiliários e função de depositário central, demonstrando que a aproximação operacional permitida pela tecnologia não dispensa a diferenciação jurídica. O agrupamento adotado neste capítulo é instrumental ao exame das funcionalidades técnicas. A separação regulatória permanece.

2. Custódia e depósito

A custódia e o depósito centralizado, em ambientes tokenizados, não são simplesmente versões digitais das atividades correspondentes no modelo tradicional, as quais operam sobre um mesmo objeto primário, que é a chave criptográfica com capacidade de movimentar o token, e convergem operacionalmente sobre um conjunto de funções técnicas compartilhadas.

A análise conjunta permite examinar essa convergência sem perder de vista que a distinção regulatória entre as atividades permanece.

Quem detém a chave controla o ativo, e esse fato redistribui parte das funções que a regulação brasileira atribui, de forma autônoma, ao custodiante e ao depositário central.

Como vimos, no modelo vigente, o depositário central recebe a titularidade fiduciária dos valores mobiliários, exerce controle centralizado sobre sua circulação e integra a cadeia de pós-negociação com os sistemas de compensação e liquidação. O custodiante, por sua vez, representa o investidor perante a infraestrutura, mantém contas individualizadas espelhadas nos registros do depositário e processa instruções de movimentação.

Um dos núcleos funcionais do depósito centralizado no modelo vigente é a restrição à prática de atos de disposição fora do ambiente do depositário,

conforme a RCVM 31/21. Essa restrição assegura a unicidade do registro e impede transferências paralelas ou duplicação de posições.

Em um ambiente tokenizado, a centralização do controle da circulação pode ser absorvida, em parte, pelo próprio protocolo da rede, que impede transferências paralelas e assegura unicidade do registro.

A guarda operacional dos tokens, por outro lado, continua exigindo a função de custódia, ressignificada como a gestão das chaves que autorizam a movimentação. A análise que segue trata dessa função comum no plano técnico, e a seção 4 retoma o reposicionamento institucional de cada atividade.

2.1.Modelos de custódia

A custódia plena (*full custody*) corresponde à modalidade em que o prestador detém integralmente o controle das chaves privadas e a capacidade técnica de movimentar os ativos do cliente. É o modelo mais próximo da custódia tradicional regulada e o que melhor se acomoda à arquitetura da RCVM 32/21.

A autocustódia (*self-custody*), no extremo oposto, devolve ao investidor o controle das chaves. Embora apresentada como expressão máxima de soberania[14], é incompatível com o modelo brasileiro de depósito centralizado obrigatório para mercados organizados e levanta questões de proteção do investidor, prevenção a perdas irreversíveis e tratamento de eventos como falecimento e sucessão.

Entre esses polos posicionam-se a custódia parcial, em que a movimentação depende da combinação de chaves detidas por mais de uma

[14] MEIJER, Carlo R. W. de. The roles of CSDs in a blockchain environment. *Journal of Securities Operations & Custody*, v. 12, n. 2, p. 167-174, 2020. O autor constata que, embora a tecnologia descentralizada permita aos indivíduos exercer a autocustódia direta de seus ativos e dissipe a cisão entre a propriedade legal e a beneficiária, grande parte dos investidores continuará a terceirizar a guarda de suas chaves privadas para depositários centrais de valores mobiliários (CSDs), visando assegurar a salvaguarda independente e mitigar o risco de perda tecnológica em um ecossistema tokenizado.

parte, e a custódia qualificada (*qualified custody*), categoria desenvolvida no debate regulatório norte-americano para identificar custodiantes sujeitos a requisitos prudenciais e operacionais específicos para ativos digitais[15].

A custódia plena preserva a estrutura de proteção do investidor, mas pode reproduzir os custos que a tokenização pretendia reduzir.

A custódia parcial, baseada em assinaturas múltiplas ou computação multipartidária, distribui o controle entre vários agentes e pode oferecer ganhos de segurança e governança, mas exige definição cuidadosa de responsabilidades em caso de falha.

A autocustódia, embora dificilmente compatível com mercados organizados, pode ter espaço em segmentos como mercados primários ou ambientes de balcão, desde que enquadrada em marco de proteção mínimo.

Por sua vez, os modelos de armazenamento são definidos pela conectividade da chave à rede[16].

---

[15] WORLD BANK. *Distributed Ledger Technology and Secured Transactions Frameworks*: A Primer. Washington, DC, 2020 (Distributed Ledger Technology & Secured Transactions: Legal, Regulatory and Technological Perspectives – Guidance Notes Series, Note 3). O relatório mapeia a flexibilização dos arranjos de custódia viabilizada pela tokenização, que transitam desde a autocustódia (*self/non-custodial*), na qual o usuário retém controle total e direto sobre suas chaves privadas e ativos digitais, até a custódia plena (*full custody*), modelo em que um terceiro gerencia essas chaves e que se consolida como preferencial para clientes institucionais por garantir a conformidade regulatória, evidenciando, adicionalmente, a necessidade de um custodiante qualificado (*qualified custodian*) para salvaguardar os ativos de referência *off-chain* no caso de tokens lastreados em ativos reais (*real world assets* – RWA).

[16] YAO, Qian. Blockchain-based New Financial Infrastructures: Theory, Practice and Regulation. Singapore: Spinger, 2022. O autor analisa as limitações estruturais da guarda de chaves privadas em ambientes desconectados da rede (*cold storage*), argumentando que a delegação exclusiva da segurança à posse do dispositivo pode se revelar catastrófica, uma vez que o extravio da chave implica a perda irreversível dos ativos digitais a ela atrelados, razão pela qual sustenta que é essencial que infraestruturas de mercado tradicionais (FMIs) forneçam um serviço de notarização e monitoramento independente capaz de garantir a recuperação de ativos desmaterializados, mitigando as limitações operacionais da custódia estruturada puramente em hardware, cabendo notar, por fim, que o arcabouço das fontes se concentra na oposição estrita entre o armazenamento online e offline (*hot* e *cold wallets*), não contendo informações e nem explorando conceitualmente as alternativas de conectividade intermediária comumente designadas no mercado como *warm wallets*.

As carteiras frias (*cold wallets*) mantêm chaves em ambientes desconectados, oferecendo maior segurança contra ataques remotos ao custo de menor disponibilidade operacional.

As carteiras quentes (*hot wallets*) mantêm chaves conectadas, viabilizando movimentação rápida com maior exposição.

As carteiras mornas (*warm wallets*) ocupam posição intermediária, com soluções híbridas que combinam essas modalidades, mantendo a maior parte dos ativos em armazenamento frio e operando fração reduzida em ambientes mais acessíveis, em lógica análoga à de gestão de caixa.

2.2.Tipologia de atividades

O ecossistema de custódia também se diversificou nos tipos de prestadores[17]. Custodiantes qualificados voltados a investidores institucionais operam com requisitos de capital, segurança e auditoria comparáveis aos de custodiantes tradicionais. Custodiantes voltados ao varejo operam em maior escala, com automação intensiva e interface direta com o investidor final.

Exchanges com custódia integrada (*embedded custody*) combinam, na mesma entidade, ambiente de negociação e guarda de ativos. Esse arranjo concentra riscos de forma incompatível com a separação funcional adotada pela regulação brasileira, e sua fragilidade ficou evidenciada nos episódios internacionais de insolvência de plataformas de criptoativos.

Por sua vez, provedores de carteiras (*wallet providers*) e empresas de infraestrutura tecnológica oferecem componentes que, sem assumir

[17] MIRDALA, Rajmund. Tokenization of Real-World Assets. *Journal of Applied Economic Sciences*, v. 20, n. 2, 2025. O autor constata que, embora o segmento de varejo acesse a fragmentação de ativos digitais predominantemente por meio de carteiras móveis, os players institucionais ainda não possuem arcabouço ou preparo para exercer a autocustódia direta, demandando inexoravelmente a atuação de bancos e fintechs como custodiantes qualificados para assegurar o armazenamento seguro dos tokens e garantir a conformidade com as regras de segregação patrimonial.

formalmente a custódia, viabilizam a guarda e a movimentação pelos clientes, em arranjos cuja qualificação regulatória ainda é objeto de debate.

2.3.Guarda e gestão de chaves

A função técnica nuclear da atividade em ambiente tokenizado é a guarda e gestão de chaves (*safekeeping and key management*), que compreende geração segura, proteção contra perda e comprometimento, mecanismos de backup e recuperação e procedimentos de rotação.

A perda de uma chave significa, em regra, a perda do ativo correspondente, sem possibilidade de reversão por instância externa. Essa propriedade introduz um risco operacional distinto do tradicional, em que a perda de um registro pode ser corrigida pela conciliação com outras bases.

No ambiente tokenizado, a criticidade dessa função se acentua no caso de chaves administrativas com poderes sobre contratos inteligentes que representam emissões inteiras de valores mobiliários, pois seu comprometimento pode afetar não apenas o titular individual, mas a integridade da emissão como um todo, função que no modelo atual é atribuída ao depositário central pelo Princípio 11 dos PFMI.

A constituição e a extinção do depósito ganham tratamento próprio em ambiente tokenizado. No modelo da RCVM 31/21, o depósito se constitui pela transferência da titularidade fiduciária ao depositário central e se extingue por solicitação do investidor ou extinção das obrigações correspondentes, com restituição da quantidade depositada.

Em uma rede DLT, esses dois momentos correspondem à emissão (*minting*) e ao resgate ou queima (*burning*) dos tokens. Essas operações têm significado jurídico equivalente à constituição e à extinção do depósito no modelo tradicional e precisam ser cercadas pelas mesmas cautelas.

O mecanismo de *minting* deve estar condicionado à verificação do lastro ou da autorização de emissão, e sua execução deve ser controlada por chaves

administrativas cuja governança reflita a responsabilidade institucional correspondente.

Por sua vez, o mecanismo de *burning* deve coexistir com regras claras de extinção e restituição, especialmente no caso de tokens lastreados em ativos externos à rede, onde a queima do token precisa ser acompanhada da entrega efetiva do ativo ou do pagamento correspondente, sob pena de reaparecimento do risco de contraparte de resgate.

2.4. Validação e autorização de transações, registro e reconciliação

A validação e autorização de transações constitui outra relevante função técnica. O custodiante verifica a legitimidade das instruções recebidas e as transforma em transações assinadas e submetidas à rede[18].

Em arranjos institucionais, a autorização envolve políticas codificadas que aplicam automaticamente limites de valor, listas de endereços autorizados (*whitelisting*)[19] e janelas de horário. Esses controles funcionam como tradução

[18] FACKLMANN, Juliana; SEVILHA, Paloma Alvares; DURAN, Camila Villard. Infraestruturas de mercado financeiro em registro distribuído: uma abordagem institucional das atividades de depositário central e de sistemas de liquidação. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, São Paulo, ano LIX, n. 180/181, p. 15-62, 2024. Disponível em: https://revistas.usp.br/rdm/article/view/217012. As autoras analisam o desenho institucional em redes DLT, ressaltando que a restrição do poder de validação de operações exclusivamente a nós autorizados constitui o mecanismo basilar para garantir a observância dos pilares de segurança, eficiência e governança. A pesquisa constata que a autorização efetiva para a movimentação de tokens exige definições exatas sobre a governança das chaves criptográficas privadas, concebendo cenários de controle nos quais o CSD retém a posse exclusiva para viabilizar a transferência unilateral segura ou, alternativamente, adota arranjos de múltiplas assinaturas, o que compartilha o poder de autorização, mas introduz novos riscos operacionais intrínsecos à complexidade da liquidação e ao processo de entrega contra pagamento (DvP).

[19] MIRDALA, Rajmund. Tokenization of Real-World Assets. *Journal of Applied Economic Sciences*, v. 20, n. 2, 2025. A pesquisa corrobora a necessidade de integrar a conformidade regulatória aos padrões abertos de tokens (a exemplo do ERC-1400 e ERC-3643) para solucionar vulnerabilidades de privacidade e segurança intrínsecas a plataformas públicas, constatando que a implementação de filtros de identidade (*identity gating*) e a adoção de arcabouços baseados em listas de permissão (*whitelisted frameworks*) são mecanismos técnico-institucionais imperativos para os desenvolvedores de infraestrutura. O autor sustenta que a automação dessas travas programáveis por meio de contratos inteligentes assegura a consistência processual das rotinas de KYC e promove a observância tempestiva de regulações

técnica das normas de conduta que, na regulação tradicional, exigem registro e rastreabilidade das instruções de movimentação.

O registro e a reconciliação de posições assumem configuração específica em ambiente tokenizado, e é nesse ponto que a aproximação operacional entre custódia e depósito se torna mais evidente.

A posição de cada investidor é, em última instância, derivável diretamente da rede, que passa a funcionar como fonte autoritativa no lugar do sistema proprietário do depositário central.

O custodiante institucional mantém registros internos que organizam a relação com o cliente, suportam auditoria e viabilizam relatórios regulatórios, mas a base comum sobre a qual todos operam é o livro-razão compartilhado.

A reconciliação deixa de ser a conferência entre bases independentes e passa a ser a verificação contínua entre os registros internos de cada participante e o estado da rede. Parte dos ciclos de conciliação diária, que hoje articulam escriturador, depositário central e custodiantes, pode ser substituída por essa verificação automatizada, desde que a governança da rede ofereça garantias de integridade equivalentes às que a regulação atual exige de cada prestador isoladamente.

2.5.Tratamento de eventos

A gestão de eventos corporativos on-chain é uma das áreas em que a tokenização promete maior simplificação. *Airdrops*, *forks*, redenominações, desdobramentos, grupamentos, migrações de protocolo e distribuições proporcionais podem ser executados diretamente sobre as posições registradas na rede, sem os fluxos atuais de comunicação entre emissor, escriturador, depositário e custodiantes.

transfronteiriças, mitigando os riscos de fragmentação de mercado e de responsabilização legal inerentes à negociação descentralizada de ativos reais tokenizados.

Essa simplificação exige decisões prévias sobre como os eventos do protocolo se traduzem em direitos do investidor e como o custodiante os reflete nos registros internos e nas comunicações ao cliente.

2.6.*Staking* e *lending*

A combinação de custódia com *staking* e empréstimo de ativos (*lending*) introduz complexidade adicional. Quando o custodiante participa, em nome do cliente, de protocolos de validação ou empréstimo, assume riscos adicionais de *slashing*, de contraparte do tomador e de liquidez do ativo emprestado. Esses riscos precisam ser segregados, comunicados e geridos, com atenção particular à informação ao cliente e à segregação patrimonial[20].

2.7.Segregação patrimonial e rastreabilidade

A segregação patrimonial e a rastreabilidade *on-chain* e *off-chain* operam em duas camadas. Na rede, a segregação pode ser implementada por endereços individualizados, contas segregadas em contratos inteligentes ou estruturas de subcontas. Fora da rede, mantém-se a estrutura tradicional de contas internas do custodiante. Detalharemos a segregação patrimonial na próxima seção, ao tratarmos das funcionalidades de liquidação.

A rastreabilidade é, em princípio, ampliada pela natureza das transações registradas na rede, mas precisa ser conciliada com obrigações de sigilo e proteção de dados. A combinação adequada dessas camadas é o que permite reproduzir a proteção patrimonial que a regulação atual obtém pela segregação em contas no depositário central, preservando a lógica da titularidade fiduciária mesmo quando o registro autoritativo migra para a rede.

A titularidade fiduciária deixa de depender exclusivamente da inscrição no sistema do depositário e passa a depender da combinação entre a

[20] CITI. *The future of post-trade*. New York: Citi Securities Services, 2025. Disponível em: https://www.citigroup.com/global/insights/the-future-of-post-trade.

representação do ativo no contrato inteligente, os endereços que o controlam e os instrumentos jurídicos que vinculam essa estrutura técnica ao regime de segregação patrimonial previsto na RCVM 31/21.

Aprofundaremos o tema em seção posterior.

2.8.Prova de reservas, ativos e passivos

A prova de reservas (*Proof-of-Reserves* - PoR) é o resultado obtido pela aplicação e verificação conjunta de dois processos complementares[21]: a prova de ativos (*Proof-of-Assets* - PoA) e a prova de passivos (*Proof-of-Liabilities* - PoL).

A prova de passivos trata especificamente da divulgação e atestação do volume total de depósitos e obrigações pendentes que a plataforma deve aos seus clientes.

O grande desafio técnico inerente a esse processo é conseguir comprovar o montante exato da dívida da *exchange* de forma publicamente auditável, mas preservando inteiramente a privacidade dos usuários. Ainda, atores mal-intencionados podem subnotificar deliberadamente o montante real de suas dívidas e passivos na tentativa de criar uma falsa ilusão de que a plataforma possui reservas plenas.

[21] BANK FOR INTERNATIONAL SETTLEMENTS (BIS); INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*. Basileia: BIS/IOSCO, 2022. Disponível em https://www.bis.org/cpmi/publ/d206.htm. O comitê estabelece que os arranjos sistemicamente importantes devem comprovar a natureza e a suficiência de seus ativos de reserva para suportar o valor do estoque total de tokens emitidos, exigindo práticas contábeis robustas e controles internos rigorosos por parte dos custodiantes para assegurar que os passivos da rede estejam integralmente cobertos e protegidos contra reivindicações de credores em cenários de insolvência. Cf. também MIRDALA, R. Tokenization of Real-World Assets. *Journal of Applied Economic Sciences*, v. 20, n. 2, 2025. A pesquisa adverte que a tokenização de ativos do mundo real e a dependência de oráculos para precificação introduzem vulnerabilidades epistêmicas nas redes de registro distribuído, concluindo que a mitigação do risco de manipulação de dados fora da rede (*off-chain*) exige a estruturação de provas de reservas baseadas em auditorias rigorosas e processos institucionais de custódia capazes de atestar indubitavelmente aos investidores que o passivo digital emitido reflete com exatidão a custódia física dos ativos subjacentes.

Em prol da verdadeira transparência e proteção, não é suficiente que uma plataforma apenas prove a posse de ativos, pois é estritamente necessário que ela confronte os seus ativos com uma prova auditável de seus passivos a fim de consolidar uma autêntica prova de reservas[22].

Merece destaque, ainda, a prova de solvência (*Proof-of-Solvency*)[23], um mecanismo de verificação abrangente projetado para avaliar a saúde financeira global de uma instituição, como uma *exchange* centralizada, demonstrando a sua real capacidade de honrar compromissos e de se manter operante no futuro. Embora o conceito englobe a prova de reservas (que verifica os ativos e passivos registrados *on-chain*), a prova de solvência vai muito além, pois considera também os ativos e obrigações da empresa que estão fora da rede (*off-chain*), além de outros fatores de risco sistêmico.

A existência conjunta de provas de ativos, passivos, reservas e solvência representa uma mudança qualitativa na forma como transparência e gestão de riscos podem ser exercidas em infraestruturas de mercado.

No modelo atual, a verificação da adequação patrimonial dos prestadores e da correspondência entre ativos custodiados e obrigações perante clientes depende de auditorias periódicas, relatórios regulatórios e supervisão externa, instrumentos que operam com defasagem temporal e cobertura amostral.

O uso de DLT permite, ao menos potencialmente, que essa verificação seja contínua, verificável por terceiros e, em alguns desenhos, executada pelo próprio investidor em relação à sua posição individual. Essa abordagem pode

[22] JI, Y.; CHUNG, I. Proof-of-Solvency: A Survey and Comparison. *IEEE Access*, v. 10, 2022. Os autores categorizam as vulnerabilidades de auditorias baseadas em Merkle-Sum Trees, apontando o risco de omissão de contas e a manipulação de passivos por entidades centrais. A pesquisa enfatiza que a *Proof of Reserves* (PoR) é insuficiente se desvinculada de uma *Proof of Liabilities* (PoL) robusta, defendendo a verificabilidade individual como requisito para mitigar a exclusão fraudulenta de obrigações no cálculo final.

[23] VIDAL-TOMÁS, David. Centralized exchanges & proof-of-solvency: The guardians of trust. *Journal of International Financial Markets, Institutions and Money*, v. 103, 102183, set. 2025. DOI: https://doi.org/10.1016/j.intfin.2025.102183.

reduzir assimetrias informacionais entre a infraestrutura, os participantes, o regulador e os investidores, e detectar em prazo mais curto situações de descasamento entre ativos e passivos que, no modelo atual, tendem a se tornar visíveis apenas em cenários de estresse.

As limitações conhecidas, especialmente a dificuldade de provar passivos sem cooperação dos clientes e a vulnerabilidade a manipulação temporal das demonstrações, não anulam o ganho funcional, mas delimitam seu alcance e reforçam que esses mecanismos são complementares à auditoria e à supervisão regulatória, não substitutos delas.

3. Liquidação

A liquidação é o ponto em que as promessas de eficiência da DLT mais se tensionam com as exigências jurídicas e regulatórias. A liquidação, no regime das IMFs, é o cumprimento definitivo das obrigações, regido pelos conceitos de entrega contra pagamento (DvP) e de finalidade. A pergunta central é *se, e em que condições, a tecnologia distribuída pode reproduzir ou aprimorar essas propriedades*.

3.1.Ativo de liquidação

O primeiro problema é o do ativo de liquidação, já mencionado anteriormente como sendo uma das decisões relevantes de arquitetura. No arranjo brasileiro, a liquidação financeira definitiva ocorre em moeda fiduciária, no âmbito do Sistema de Pagamentos Brasileiro (SPB).

Uma infraestrutura tokenizada na qual, de um lado, temos o ativo representado em rede distribuída, mas de outro lado, dependa de liquidação financeira em sistema externo, mantém o descasamento temporal e operacional entre as duas pernas. Se a liquidação for feita em moeda fiduciária por meios

tradicionais, persistem janelas de exposição, necessidade de coordenação entre sistemas e perda de boa parte do potencial de atomicidade[24].

Esses inconvenientes podem ser parcialmente contornados por mecanismos de *hold-to-settle*, sincronizados com a transferência tokenizada[25], ou pela introdução, na própria rede, de representações tokenizadas de moeda, sejam depósitos tokenizados emitidos por instituições autorizadas, stablecoins lastreadas em ativos seguros ou moedas digitais de banco central.

A emissão e negociação de tokens, articuladas com liquidação em stablecoins ou em moedas digitais de banco central, introduzem ganhos adicionais. A representação tokenizada do ativo permite programar o ciclo de

[24] FACKLMANN, Juliana; SEVILHA, Paloma Alvares; DURAN, Camila Villard. Infraestruturas de mercado financeiro em registro distribuído: uma abordagem institucional das atividades de depositário central e de sistemas de liquidação. *Revista de Direito Mercantil, Industrial, Econômico e Financeiro*, São Paulo, ano LIX, n. 180/181, p. 15-62, 2024. Disponível em: https://revistas.usp.br/rdm/article/view/217012. As autoras examinam as particularidades da implementação do mecanismo de Entrega contra Pagamento (*Delivery versus Payment* - DvP) em redes de registro distribuído (DLT), argumentando que a combinação de infraestruturas *on-chain* para a entrega do ativo com sistemas legados *off-chain* para o pagamento (*cash leg*) introduz fricções estruturais e riscos de falha na liquidação, postulando, assim, a necessidade técnica de emissão de equivalentes monetários no próprio ambiente distribuído, designados como tokens monetários (como stablecoins e moedas digitais de bancos centrais - CBDCs), para garantir a liquidação atômica e simultânea das obrigações.

[25] EVERETT, Steve; CALITZ, Andre; GREYLING, Jean. The case for a 'sovereign' distributed securities depository for securities settlement. *Journal of Securities Operations & Custody*, Londres, v. 9, n. 3, p. 269-292, 2017. Os autores constatam que a efetivação segura do modelo DvP descentralizado demanda o emprego estrito de contratos inteligentes projetados para manter os ativos tokenizados retidos em estado de *escrow*, assegurando que moeda e o título devem permanecer rigidamente bloqueados na rede até que o pareamento integral das chaves criptográficas destrave a liquidação simultânea, o que mitiga a dependência de infraestruturas legadas apartadas e blinda os investidores contra o risco de principal. Cf. também PINHO, Pedro Duarte. *Regulação das infraestruturas de mercado financeiro*: estudo sobre a influência do soft-law internacional na construção do arcabouço brasileiro. 2025. Dissertação (Mestrado em Direito e Desenvolvimento) - Escola de Direito de São Paulo, Fundação Getulio Vargas, São Paulo, 2025. O autor descreve que o mecanismo de Entrega contra Pagamento (*Delivery versus Payment* - DvP) exige estruturalmente uma etapa preliminar de bloqueio e reserva dos ativos em nome do vendedor antes da liquidação financeira, um arranjo de imobilização prévia (hold-to-settle) que vem sendo transposto para as redes de registro distribuído (DLT), como ilustrado em projeto piloto da Depository Trust & Clearing Corporation (DTCC) que empregou bloqueios em duas fases para reter tokens de valores mobiliários e moedas digitais de banco central (CBDCs), condicionando a liberação algorítmica e a transferência atômica dos ativos à estrita satisfação das obrigações financeiras da contraparte.

eventos corporativos, marcar gravames com eficácia operacional imediata e viabilizar liquidação atômica com a perna financeira.

A escolha do ativo de liquidação, contudo, condiciona o perfil de risco e o tratamento regulatório.

As stablecoins privadas, tipicamente lastreadas em ativos seguros e emitidas por entidades sujeitas a alguma forma de regulação, oferecem disponibilidade e flexibilidade operacional[26]. Carregam, contudo, o risco de contraparte de resgate já mencionado. Dependem da qualidade do lastro, da governança do emissor e da efetividade da supervisão a que ele se submete. Episódios de descolamento da paridade observados internacionalmente demonstram que essa modalidade não é, por si, equivalente a moeda de banco central.

Por seu turno, as moedas digitais de banco central podem ser categorizadas em duas vertentes[27]. As CBDCs de varejo (*retail*) destinam-se ao público em geral e funcionam como representação digital do dinheiro em

[26] O atual mercado de stablecoins opera em uma rede fragmentada "muitos-para-muitos", onde as transações são liquidadas de forma bilateral. Isso exige que carteiras e provedores estabeleçam conexões diretas com múltiplos emissores em diferentes blockchains, gerando complexidade, atritos operacionais e incerteza jurídica sobre os termos dos contratos. A confiança, nesse cenário, depende da credibilidade e da solvência das reservas do emissor. Cf. COCCO, Alessandro. *Toward a normative framework for a payment stablecoin financial market infrastructure*. SSRN, 2025. Disponível em: https://doi.org/10.2139/ssrn.5723064.

[27] CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE (CCAF). *Digital Public Infrastructure and Digital Financial Services*: Convergence, Landscape and Regulatory Considerations. Cambridge, 2025. Disponível em https://www.jbs.cam.ac.uk/2025/global-regulatory-trends-for-digital-public-infrastructure/. O relatório estabelece a distinção estrutural dos arranjos de moedas digitais de bancos centrais (CBDCs), definindo as CBDCs de varejo como passivos diretos acessíveis ao público em geral, em dinâmica equivalente à do papel-moeda, enquanto as CBDCs de atacado têm sua emissão e participação restritamente franqueadas a instituições financeiras selecionada. Cf. também: BUCKLEY, Ross P.; ARNER, Douglas W.; ZETZSCHE, Dirk A. Electronic payments, stablecoins, and central bank digital currencies. In: *FINTECH*. Cambridge: Cambridge University Press, 2023. Disponível em https://doi.org/10.1017/9781009086943.017. Os autores enquadram stablecoins como instrumentos privados de pagamento e liquidação que replicam, em ambiente DLT, funções monetárias sem acesso direto à base monetária, ao passo que CBDCs representam passivos do banco central, aptos a operar como ativo de liquidação final em sistemas tokenizados, com implicações diretas para desenho de infraestruturas de mercado, governança e regulação da liquidação.

espécie, com implicações para o sistema bancário, a privacidade e a transmissão da política monetária. As CBDCs de atacado (*wholesale*) são de uso restrito a instituições financeiras e infraestruturas, voltadas especificamente à liquidação entre essas entidades.

Para IMFs, a modalidade de atacado é a alternativa mais direta, na medida em que oferece finalidade jurídica equivalente à da moeda de banco central tradicional, sem os efeitos sistêmicos mais amplos da modalidade de varejo.

A diferença entre liquidação em stablecoins e em CBDCs concentra-se em três dimensões[28].

Em primeiro lugar, a natureza do ativo. A stablecoin é uma obrigação privada; a CBDC é moeda fiduciária com curso legal.

Em segundo lugar, a liquidação em moeda de banco central oferece finalidade plena, enquanto a liquidação em stablecoin introduz a dependência da solidez do emissor.

Em terceiro lugar, o tratamento prudencial. A exposição a stablecoins tende a ser tratada como exposição de crédito ao emissor, ao passo que a exposição a CBDC equivale, do ponto de vista prudencial, à exposição a moeda soberana.

[28] A experiência europeia evidencia a tendência de integração entre plataformas DLT privadas e infraestruturas de liquidação em moeda de banco central, por meio de modelos "*bridge*" ou de *ledger* compartilhado, nos quais CBDCs funcionam como ativo de liquidação que ancora transações tokenizadas, ao contrário de stablecoins, cuja liquidação permanece dependente de conversibilidade externa e não garante integração plena com sistemas de liquidação sistêmicos – cf. EUROPEAN CENTRAL BANK. *Preparing the future of payments and money: the role of central bank money*. Frankfurt: ECB, 2025 (Keynote speech by Piero Cipollone, Member of the Executive Board of the ECB). Disponível em https://www.ecb.europa.eu/press/key/date/2025/html/ecb.sp250926~e856d2e386.en.html.

Dimensão	Stablecoin	CBDC de atacado
Natureza do ativo	Obrigação privada	Moeda fiduciária com curso legal
Finalidade	Depende da solidez do emissor	Finalidade plena
Tratamento prudencial	Exposição de crédito ao emissor	Exposição a moeda soberana

Figura 1 – Liquidação em stablecoins e em CBDCs

Elaboração própria.

Essas diferenças não anulam o papel das stablecoins, que podem operar como instrumento intermediário e oferecer ganhos de eficiência, mas demonstram por que os bancos centrais de diversas jurisdições têm desenvolvido projetos de CBDC de atacado voltados à liquidação em infraestruturas tokenizadas.

Para a regulação brasileira, a articulação entre eventuais infraestruturas baseadas em DLT supervisionadas pela CVM e o ativo de liquidação a ser utilizado é uma das decisões institucionais mais relevantes e depende diretamente da evolução do projeto Drex e de sua interação com o SPB.

3.2.Finalidade da liquidação (*settlement finality*)

O segundo problema diz respeito à finalidade da liquidação (*settlement finality*). Como vimos, a finalidade exigida pela regulação prudencial e pelos PFMI é determinística, não probabilística[29].

[29] De acordo com o Princípio 8 dos PFMI, finalidade da liquidação é a transferência irrevogável e incondicional de um ativo ou o efetivo cumprimento de uma obrigação financeira, exigindo que o arcabouço jurídico e as regras da infraestrutura definam claramente o momento exato em que a transação se torna final, de modo a afastar riscos de reversão associados a regras de insolvência.

Uma transação liquidada não pode estar sujeita a reversão por reorganização da cadeia ou por qualquer outro mecanismo de natureza estatística.

Redes públicas baseadas em consenso probabilístico oferecem finalidade que se aproxima assintoticamente do determinismo, mas nunca o atinge plenamente, o que é incompatível com o regime jurídico de liquidação definitiva.

Redes permissionadas operadas com mecanismos de tolerância bizantina a falhas oferecem finalidade determinística no momento do consenso, propriedade que se aproxima do regime exigido pelas IMFs reguladas[30].

Logo, a escolha do mecanismo de consenso é condicionada pela própria possibilidade de qualificar a infraestrutura como sistema de liquidação.

Esse ponto se conecta com uma deficiência específica da aplicação acrítica de validade jurídica a registros determinísticos na rede. O fato de uma transação tornar-se imutável no protocolo não significa que ela tenha eficácia jurídica externa equivalente. Quando o token representa um ativo cuja existência depende de mundo externo à rede, a integridade do registro convive com o risco de que a contraparte responsável pela conversão entre o token e o ativo subjacente não honre essa obrigação.

Esse risco, frequentemente designado como risco de contraparte de resgate (*redemption counterparty risk*), aparece de forma mais evidente nas

[30] A mecânica de obtenção da finalidade varia substancialmente conforme o desenho da DLT, constatando que certas redes não permissionadas admitem a reversão temporária de atualizações, o que conflita com as necessidades institucionais de segurança e impulsiona as entidades financeiras a priorizarem tecnologias restritas para garantir a efetiva irrevogabilidade dos ativos liquidados. CF. PINNA, Andrea; RUTTENBERG, Wiebe. *Distributed ledger technologies in securities post-trading*: revolution or evolution? Frankfurt am Main: European Central Bank, 2016. Disponível em https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

stablecoins lastreadas em moeda fiduciária[31]. Nesse caso, a propriedade do token é tecnicamente irrevogável, mas o valor econômico depende da capacidade do emissor de honrar o resgate ao par. A liquidação no protocolo é determinística, mas a liquidação econômica permanece sujeita à solidez do emissor.

O mesmo problema reaparece em qualquer ativo tokenizado cuja exigibilidade dependa de instituição externa à rede. A consequência regulatória é que a finalidade técnica da rede, embora condição necessária, não é suficiente. É preciso que a estrutura institucional do ativo de liquidação assegure que a transação determinística no protocolo corresponda a uma transação economicamente irreversível. Por essa razão, BIS e IOSCO enfatizam que é imperativa a adoção de mecanismos que assegurem a incondicionalidade da transferência independentemente de instabilidades no registro[32].

3.3.Liquidação atômica

A liquidação atômica é a principal promessa funcional da DLT nesse campo[33], consistindo na execução simultânea e indivisível das duas pernas de uma operação, de modo que ou ambas se concretizam, ou nenhuma delas.

---

[31] ZENG, James Si. *Whither central clearing counterparties*? Counterparty risk in stablecoin-based securities settlement. University of Hong Kong Faculty of Law Research Paper No. 2025/31, 2025. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5737822.

[32] BANK FOR INTERNATIONAL SETTLEMENTS (BIS); INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*. Basileia: BIS/IOSCO, 2022. Disponível em https://www.bis.org/cpmi/publ/d206.htm.

[33] BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *Tokenisation in the context of money and other assets*. Basel, 2023. Disponível em: https://www.bis.org/cpmi/publ/d225.pdf. O relatório insere a liquidação atômica no núcleo das arquiteturas DLT ao destacar que a tokenização permite a execução simultânea das pernas de ativos e pagamentos em um ambiente programável único, eliminando a necessidade de reconciliação entre sistemas e reduzindo a complexidade operacional, ao mesmo tempo em que reforça o papel de ativos de liquidação seguros, como a moeda de banco central, para garantir finalização e neutralidade do sistema. Cf. também OECD. *Tokenisation of assets and distributed ledger technologies in financial markets*. Paris, 2024. Disponível em: https://www.oecd.org/en/publications/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_40e7f217-en.html. A análise da OCDE

Em comparação com os modelos clássicos de DvP, corresponde a uma versão radicalizada do DvP 1, com a vantagem adicional de dispensar coordenação entre dois sistemas para garantir a simultaneidade.

As vantagens são potencialmente significativas[34], entre elas a eliminação do risco de principal, a redução do capital imobilizado em garantias e o encurtamento do ciclo entre negociação e liquidação. Adicionalmente, em teoria, o uso de DLT permite que a liquidação contínua e ininterrupta funcione 24 horas por dia, 7 dias por semana, rompendo as barreiras de fusos horários dos mercados tradicionais.

Os inconvenientes, porém, não podem ser ignorados[35]. A liquidação atômica em base bruta opera operação a operação, dispensando a compensação

---

reconhece a liquidação atômica como uma das principais promessas da DLT ao permitir ciclos de liquidação instantâneos e programáveis, mas destaca limitações relevantes, como impactos sobre gestão de liquidez, ausência de evidência empírica em larga escala e desafios jurídicos relacionados à finalização e à correspondência entre token e ativo subjacente, indicando que seus benefícios dependem de integração sistêmica e padronização institucional.

[34] COLLE, Luke. Reaching for the moon: an analysis of real-time securities clearing and settlement in light of emerging blockchain technologies. *Virginia Law & Business Review*, v. 16, 2022; CITI. *The future of post-trade*. New York: Citi Securities Services, 2025. Disponível em: https://www.citigroup.com/global/insights/the-future-of-post-trade.

[35] Para uma leitura com ceticismo a respeito do uso de DLT e seus riscos, cf. MILKAU, U. Will tokenisation deliver efficiency? And what kind? *Journal of Securities Operations & Custody*, v. 17, n. 1, p. 79-94, dez. 2024. De acordo com o autor, a verdadeira eficiência não resulta da simples representação digital de ativos do mundo real em blockchain ou da programabilidade de um sistema de computador, mas sim da integração e da sincronização de processos dentro das infraestruturas do mercado financeiro. os benefícios desejados da digitalização podem ser plenamente alcançados por meio de sincronização sem DLT, sem que o sistema precise se basear em tokens. Uma crítica mais ácida pode ser encontrada no ensaio MONAHAN, Ken. *Steampunk settlement: deploying futuristic technology to achieve an anachronistic result*. Greenwich Associates, 2019. Disponível em: https://www.greenwich.com/sites/default/files/files/reports/Steampunk-Settlement.19-2018.pdf. Para o autor, o uso de DLT para alcançar a liquidação instantânea (T+0) representa um retrocesso prático e histórico. A conclusão central é que a liquidação em tempo real exige o pré-financiamento (*pre-funding*) de todas as operações, o que "volta o relógio" para um breve período no ano de 1584, quando o Senado de Veneza exigiu a mesma prática para as negociações feitas através do Banco di Rialto. Segundo o relatório, os defensores da tecnologia blockchain que buscam substituir o sistema atual estão, na verdade, argumentando a favor da implantação caríssima de uma tecnologia futurista com o único propósito de alcançar um "resultado medieval". Esse conceito, que inspira o termo *Steampunk* no título do artigo (a mistura de alta tecnologia com o passado), baseia-se na constatação de que a liquidação instantânea sacrifica a eficiência construída pelos mercados modernos.

multilateral que constitui um dos principais ganhos de eficiência das contrapartes centrais.

Esse modelo aumenta a demanda por liquidez intradiária, exige pré-financiamento integral e pode ser pouco adequado a mercados de alto giro com participantes que dependem de compensação para gerir suas posições.

Ainda, a enorme volume de negociações em tempo real poderia aumentar a ocorrência de falhas nas transações, impulsionadas por erros de instrução ou confusões de comunicação.

Os fundos mútuos de garantia e as cascatas de salvaguardas das CCPs não encontram equivalente direto em arranjos puramente atômicos. A escolha entre liquidação atômica e modelos que preservem a compensação multilateral é uma escolha entre eliminar o risco de principal por design e preservar eficiência de capital e mecanismos de mutualização de risco[36].

Soluções intermediárias, como liquidação atômica em janelas ou redes que combinem compensação multilateral com liquidação atômica do saldo líquido, surgem como tentativas de reconciliar essas propriedades.

3.4.Síntese

A liquidação em ambiente tokenizado oferece ganhos condicionados a escolhas arquiteturais específicas. A obtenção desses ganhos depende da combinação entre mecanismo de consenso adequado à finalidade (*settlement finality*), ativo de liquidação que preserve a equivalência econômica da liquidação técnica, modelo que equilibre atomicidade e eficiência de capital, e

[36] PLATA, Rafael et al. Decentralised clearing? An assessment of the impact of DLTs on CCPs. *Journal of Securities Operations & Custody*, vol. 16(3), pages 227-246, jun. 2024. De acordo com os autores, as novas tecnologias não alteram a natureza fundamental da gestão de risco que ancoram o propósito dessas instituições. Por exemplo, O risco futuro potencial de um contrato de derivativo exige mecanismos contínuos de cálculo de risco, chamadas de margem e gestão de garantias, funções que justificam estruturalmente a figura de um intermediário central.

desenho institucional que reproduza ou substitua as funções das contrapartes centrais em situações de estresse.

4. Gestão de garantias

A gestão de garantias é uma das atividades mais onerosa em termos de custo de coordenação entre infraestruturas e participantes[37]. No modelo vigente, garantias são depositadas, avaliadas, marcadas a mercado, substituídas e liberadas por meio de fluxos que envolvem custodiantes, contrapartes centrais, depositários e, não raro, registradoras. Cada um desses agentes mantém seus próprios registros, o que obriga a ciclos recorrentes de reconciliação entre bases independentes.

A imobilização de colateral tende a ser conservadora, porque a informação sobre a posição atualizada de cada participante não está disponível em tempo real (ou tempestivamente) para todos os envolvidos. O resultado é capital inerte acima do necessário, alocação subótima de garantias e custos operacionais que se acumulam ao longo da cadeia.

A introdução de um livro-razão compartilhado pode alterar essa dinâmica. Quando todos os participantes relevantes têm acesso ao mesmo registro, a reconciliação entre bases independentes perde a razão de ser. A posição de cada agente, os gravames constituídos, o valor atualizado dos ativos oferecidos em garantia e o estado das obrigações cobertas passam a ser verificáveis a partir de uma fonte comum[38].

---

[37] GLOBAL FINANCIAL MARKETS ASSOCIATION. The impact of distributed ledger technology in capital markets. Washington: GFMA, 2025. Disponível em: https://www.gfma.org/wp-content/uploads/2025/08/2.-exec-sum-impact-of-dlt-in-cap-mkts-final.pdf. O estudo identifica a gestão de colateral como um dos casos de uso mais promissores da DLT, destacando que *smart contracts* permitem automação do ciclo de vida das garantias, desde a alocação até a substituição e liberação, com ganhos de eficiência operacional e redução de risco de reconciliação, mas exige robustos mecanismos de governança, validação de código e resiliência operacional para assegurar equivalência funcional às infraestruturas tradicionais.

[38] AVGOULEAS, Emilios; KIAYIAS, Aggelos. The promise of blockchain technology for global securities and derivatives markets: the new financial ecosystem and the "holy grail" of systemic

Contratos inteligentes podem automatizar a liberação de colateral quando a obrigação subjacente é cumprida, a substituição de garantias quando o valor de mercado cai abaixo de determinado limiar, e a recomposição de margens sem intervenção manual[39].

Em tese, isso permite operar com níveis de colateral mais próximos do risco efetivo, liberando capital para outros usos.

A tese de que a maior redução de custos virá da eliminação de processos redundantes de reconciliação, e não da eliminação de atores, deve ser analisada com cuidado. Ela é plausível para fluxos rotineiros, nos quais a redundância decorre da fragmentação de bases de dados e não de escolhas regulatórias deliberadas. Nesses casos, o livro-razão compartilhado elimina trabalho duplicado sem alterar a estrutura institucional do mercado.

A ressalva necessária é que nem toda reconciliação é redundante. Parte dos processos de conciliação diária existe para detectar inconsistências entre camadas funcionais distintas, como a correspondência entre titularidade plena no escriturador e titularidade fiduciária no depositário central. Essa correspondência cumpre função de controle que não desaparece simplesmente porque os dados passam a residir em uma rede compartilhada.

---

risk management. *European Business Organization Law Review*, v. 20, n. 1, p. 1-32, 2019. Disponível em: https://doi.org/10.1007/s40804-019-00133-3. Para os autores, sistemas DLT podem aumentar drasticamente a visibilidade das posições de risco, criando um ecossistema financeiro mais diversificado. O ganho de controle pelos investidores e o aumento da transparência pós-negociação serão forças importantes para conter a especulação excessiva movida por alavancagem.

[39] A adoção de DLT permite a codificação de regras de margem diretamente em contratos inteligentes, o que automatiza as chamadas de margem (margin calls) e os ajustes algorítmicos de precificação, ampliando o controle dos investidores institucionais sobre as garantias fornecidas e mitigando os riscos sistêmicos inerentes à reutilização excessiva de colateral (collateral re-use) no mercado tradicional. Cf. AVGOULEAS, Emilios; KIAYIAS, Aggelos. The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment. *European Business Organization Law Review*, v. 20, p. 81-110, 2019. Disponível em: https://doi.org/10.1007/s40804-019-00133-3.

A eliminação da reconciliação só é segura quando o livro-razão compartilhado efetivamente substitui as bases anteriores como fonte soberana, e quando a governança da rede oferece garantias equivalentes às que a regulação hoje impõe a cada prestador isoladamente.

Os riscos e efeitos colaterais da gestão de garantias em DLT merecem atenção equivalente. A automação por contrato inteligente transfere para o código decisões que, no modelo atual, passam por avaliação humana ou por sistemas com margem de discricionariedade. Chamadas de margem automatizadas, por exemplo, podem gerar efeitos pró-cíclicos se o contrato executar liquidações forçadas em resposta a variações bruscas de preço, sem mecanismos de amortecimento ou intervenção temporária[40].

Por fim, a transparência do livro-razão, embora benéfica para a verificação das posições, pode expor informações competitivamente sensíveis se o desenho de privacidade da rede for insuficiente. Participantes que consigam observar os níveis de colateral e as posições de contrapartes podem explorar essas informações de formas que a regulação de mercado procura coibir.

[40] FINANCIAL STABILITY BOARD (FSB). *The financial stability implications of tokenisation*. Basel: FSB, 2024. Disponível em: https://www.fsb.org/uploads/P221024-2.pdf. O FSB destaca que a programabilidade de *smart contracts* altera a dinâmica da gestão de colateral ao automatizar chamadas de margem, liquidações e reutilização de garantias, mas pode amplificar riscos de liquidez e interconectividade, especialmente quando o mesmo colateral pode sustentar múltiplas exposições em cadeias complexas. No mesmo sentido: AQUILINA, Matteo et al. *Cryptocurrencies and decentralised finance*: functions and financial stability implications. BIS Papers, n. 156. Basel: BIS, 2025. Disponível em: https://www.bis.org/publ/bppdf/bispap156.htm O BIS analisa a gestão de colateral em protocolos baseados em *smart contracts* como um processo automatizado e frequentemente sobrecolateralizado, destacando que a ausência de discricionariedade e a rigidez do código amplificam riscos pró-cíclicos, especialmente em cenários de estresse, nos quais liquidações automáticas podem gerar espirais de desvalorização e pressão sobre a liquidez, sem mecanismos institucionais de contenção comparáveis aos existentes em infraestruturas tradicionais

5. Proteção patrimonial via segregação e outros meios

5.1. Segregação patrimonial

A segregação patrimonial é o outro eixo relevante da proteção do investidor nesse ambiente[41]. No modelo regulatório brasileiro, os ativos dos investidores são segregados do patrimônio do custodiante e do depositário central, protegidos por titularidade fiduciária e mantidos em contas individualizadas. Essa arquitetura assegura que, em caso de insolvência do prestador de serviço, os ativos dos clientes não se confundam com a massa falida.

Em ambientes tokenizados, a segregação pode ser implementada de duas formas[42].

A segregação individual atribui a cada investidor um endereço ou conjunto de endereços próprios na rede, nos quais seus ativos ficam registrados de modo independente dos demais.

A segregação coletiva, ou *omnibus*, reúne os ativos de múltiplos investidores em um mesmo endereço ou contrato inteligente, cabendo ao custodiante manter, em registros internos, a identificação da parcela de cada cliente.

A segregação individual oferece vantagens evidentes em termos de transparência e proteção contra insolvência. Cada investidor pode verificar

[41] FINANCIAL ACTION TASK FORCE. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris, 2021. Disponível em: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf. A orientação estabelece a segregação d e ativos de clientes como elemento central da mitigação de riscos em VASPs, exigindo a separação entre recursos próprios e de clientes como mecanismo de proteção contra insolvência e uso indevido, ao mesmo tempo em que evidencia a necessidade de controles internos e registros contábeis que assegurem a rastreabilidade e identificação individual dos ativos em ambientes digitais.

[42] PRIEM, Randy. Asset segregation at CSDs: protecting investors with a level playing field. *European Business Law Review*, v. 31, n. 5, 2020. Disponível em https://doi.org/10.54648/EULR2020034.

diretamente na rede que seus ativos estão sob o endereço correto e não foram movimentados sem autorização. Em caso de falência do custodiante, a identificação dos ativos de cada cliente não depende da integridade dos registros internos da entidade insolvente, pois o próprio livro-razão da rede já os individualiza.

Essa propriedade reforça o conceito de *bankruptcy remoteness*[43] de forma estrutural, por desenho tecnológico, e não apenas por imposição normativa.

A segregação *omnibus*, por outro lado, é operacionalmente mais leve, exige menor número de transações na rede e pode reduzir custos de *gas* ou taxas de validação. Ela é também o modelo predominante na custódia tradicional de valores mobiliários em diversos países[44], onde a individualização

[43] *Bankruptcy remoteness* é um atributo estrutural de operações de securitização que isola ativos do risco de insolvência do originador, permitindo que investidores precifiquem os títulos com base na qualidade dos ativos e não na solvência do emissor, ao mesmo tempo em que demonstram que tal isolamento pode gerar efeitos econômicos ambíguos, como incentivos a liquidações ineficientes quando ativos essenciais são retirados do alcance do processo falimentar. Cf. AYOTTE, Kenneth M.; GAON, Stav. Asset-Backed Securities: Costs and Benefits of "Bankruptcy Remoteness". New York: Federal Reserve Bank of New York, 2006. Disponível em: https://www.newyorkfed.org/medialibrary/media/research/conference/2006/cffi/Ayotte.pdf. Cf. também: AMERICAN BAR ASSOCIATION. *Bankruptcy Remoteness*: A Summary Analysis. Chicago, 2022. Disponível em: https://www.americanbar.org/groups/business_law/resources/business-lawyer/2022-fall/bankruptcy-remoteness-summary-analysis/. O estudo sistematiza os elementos jurídicos da *bankruptcy remoteness*, enfatizando o papel de veículos de propósito específico, da caracterização de "true sale" e da mitigação do risco de substantive consolidation como instrumentos para segregar ativos e limitar o alcance da jurisdição falimentar, ainda que reconheça a possibilidade de intervenção judicial que relativize tais estruturas.

[44] PRIEM, Randy. Asset segregation at CSDs: protecting investors with a level playing field. *European Business Law Review*, v. 31, n. 5, p. 475-505, 2020. Disponível em https://doi.org/10.54648/EULR2020034. O autor assinala que, nas cadeias de custódia de valores mobiliários, a segregação *omnibus* constitui modelo amplamente utilizado, no qual ativos de múltiplos clientes são mantidos em uma única conta ao nível do depositário central ou do custodiante, sendo a individualização assegurada por registros internos e reconciliações contábeis dos intermediários, o que preserva direitos econômicos equivalentes sob determinadas condições jurídicas e reduz custos operacionais. Cf. também: EUROPEAN CENTRAL SECURITIES DEPOSITORIES ASSOCIATION. CSDs, asset segregation, and custody services under UCITS and AIFMD. Bruxelas: ECSDA, 2016. Disponível em: https://ecsda.eu/archives/5250. O documento evidencia que, no nível das infraestruturas centrais, os participantes podem optar por contas *omnibus* ou individualizadas, sendo comum que a granularidade da segregação não alcance o investidor final, sobretudo em cadeias

se dá nas contas internas do custodiante e do depositário, não necessariamente no nível mais baixo da infraestrutura.

O risco, em ambiente tokenizado, é que a segregação *omnibus* reproduza precisamente a dependência que a DLT poderia ajudar a superar. Se o custodiante falir e seus registros internos estiverem corrompidos ou incompletos, a identificação dos ativos de cada cliente torna-se tão problemática quanto no modelo tradicional, apesar de os ativos estarem registrados em rede distribuída.

Contratos inteligentes podem reforçar a proteção patrimonial mesmo em arranjos *omnibus*, por meio de regras codificadas que impeçam a movimentação dos ativos para fins não autorizados, que limitem a concentração de ativos sob controle de um único operador e que registrem, de forma imutável, cada alteração no saldo atribuído a cada cliente.

Essas regras funcionam como camada adicional de controle, mas não substituem a necessidade de governança institucional sobre o contrato e de mecanismos de intervenção em situações excepcionais, como decisões judiciais ou procedimentos de liquidação extrajudicial.

5.2.Seguros

A proteção patrimonial em ambiente tokenizado também se articula com a cobertura securitária[45]. No ecossistema de ativos digitais, três modalidades de seguro ganharam relevância.

O *crime insurance* cobre perdas decorrentes de atos ilícitos de funcionários ou terceiros, como desvio de chaves privadas ou manipulação de

internacionais, nas quais a identificação detalhada permanece nos sistemas internos dos custodiantes e não no *ledger* do CSD.

[45] INTERNATIONAL ASSOCIATION OF INSURANCE SUPERVISORS. *Global Insurance Market Report* (GIMAR). Basel: IAIS, 2023. Disponível em: https://www.iais.org/uploads/2023/12/Global-Insurance-Market-Report-2023.pdf.

sistemas internos. O *cyber insurance* cobre perdas decorrentes de ataques cibernéticos, invasões de sistemas e exploração de vulnerabilidades.

A distinção entre *cyber insurance* e *crime insurance* é sistematizada pela diferenciação entre perdas intangíveis e indiretas associadas a sistemas e dados, no primeiro caso, e perdas diretas e tangíveis associadas a apropriação indevida de ativos, no segundo, sendo comum a sobreposição parcial em eventos como fraude eletrônica e engenharia social, o que demanda estruturas combinadas de cobertura[46].

O seguro *specie* cobre a perda direta dos ativos digitais sob custódia, independentemente da causa. Historicamente, esta modalidade é utilizada para itens de alto valor portáteis, como metais preciosos, joias e numerário, e foi recentemente adaptada para criptoativos mantidos em *cold storage*. Assim, as chaves são equiparadas a "bens tangíveis"[47].

A disponibilidade dessas coberturas no mercado segurador é ainda restrita, com prêmios elevados e limites de indenização frequentemente inferiores ao valor dos ativos sob custódia. Essa limitação faz com que o seguro funcione, na prática, como mecanismo complementar de proteção, e não como substituto da segregação patrimonial, da governança institucional e da supervisão regulatória.

---

[46] EUROPEAN CENTRAL BANK. *Cyber resilience oversight expectations for financial market infrastructures*. Frankfurt: ECB, 2018. Disponível em: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf. O ECB reconhece que seguros podem integrar o arcabouço de gestão de risco operacional de FMIs, mas ressalta que sua função é subsidiária em relação a controles preventivos e planos de continuidade, sendo inadequado tratar seguros como substituto de resiliência operacional, sobretudo em ambientes digitais e interconectados.

[47] KESHANI, Azmina. Safeguarding Digital Assets: A Framework for Evaluating Custodians. In: DE SILVA, Sam et al. (Eds.). *Expert Essentials*. Oxford: Oxford Law Pro, 2025. Disponível em: https://academic.oup.com/oxford-law-pro/edited-volume/59931/chapter/512683517. O trabalho situa a cobertura securitária como componente essencial da infraestrutura de custódia institucional, observando que a fragmentação regulatória entre jurisdições repercute diretamente sobre a viabilidade e o escopo das apólices disponíveis, na medida em que a qualificação do ativo como propriedade constitui pressuposto tanto para a incidência de estruturas fiduciárias quanto para a aplicabilidade de coberturas do tipo *specie*.

5.3.Formadores de mercado e *exchanges* descentralizadas

Os formadores de mercado automatizados (*automated market makers* – AMMs) e as *exchanges* descentralizadas (DEX) representam um modelo alternativo para a provisão de liquidez e a intermediação de risco.

No modelo tradicional, a liquidez é oferecida por intermediários que mantêm posições próprias, operam *spreads* e assumem risco de estoque, sujeitos a requisitos regulatórios de capital, conduta e dever de melhor execução.

Nas DEX, a liquidez é provida por *pools* de ativos depositados por provedores que não são, necessariamente, intermediários regulados. A formação de preço ocorre por algoritmo, tipicamente uma função matemática que relaciona as quantidades dos dois ativos no *pool* e ajusta o preço conforme a proporção se altera. O investidor negocia diretamente contra o *pool*, sem intermediário identificável e sem livro de ofertas[48]. Esse modelo elimina a necessidade de intermediário para a execução do negócio, o que reduz custos de intermediação e amplia o acesso à provisão de liquidez.

Ao mesmo tempo, introduz riscos próprios. A perda impermanente (*impermanent loss*) afeta provedores de liquidez quando o preço relativo dos ativos no *pool* diverge do preço de mercado. O *slippage* pode ser significativo em *pools* com baixa liquidez[49].

Adicionalmente, a ausência de intermediário regulado elimina a camada de proteção que a regulação de conduta oferece ao investidor, como *suitability*,

[48] COSTA, Isac Silveira da. A sorte favorece os bravos, mas não os tolos - DeFi: escopo, riscos e desafios regulatórios das finanças descentralizadas. In: GOMES, Daniel de Paiva; GOMES, Eduardo de Paiva; CONRADO, Paulo Cesar (coords.). *Criptoativos, tokenização, blockchain e metaverso*. São Paulo: Thomson Reuters, 2022.

[49] DEL MONTE, Ignacio Ariel; DE LUCIO, Juan José; SICILIA URBAN, Miguel Ángel. Current Understanding of Impermanent Loss Risk in AMMs. *Blockchain: Research and Applications*, 2025. Disponível em: https://doi.org/10.1016/j.bcra.2025.100360; LEE, Gyu M.; KIM, Hyoung Joong. Impermanent Loss Mitigation for Decentralized Exchanges through Optimization. *International Journal of Industrial Engineering*, 2024. Disponível em: https://doi.org/10.23055/ijietap.2024.31.6.10691.

melhor execução e mecanismos de ressarcimento. E a governança dos protocolos de DEX, frequentemente descentralizada e baseada em votação de detentores de tokens de governança, não encontra equivalente funcional nos mecanismos de autorregulação e supervisão estatal previstos na RCVM 135/22.

A relevância dos AMMs e DEX para a discussão regulatória brasileira não está na substituição integral dos mercados organizados – hipótese que as exigências de proteção do investidor e integridade de mercado tornam improvável no curto prazo –, mas sim na possibilidade de que elementos dessa arquitetura sejam incorporados a mercados regulados, por exemplo na forma de *pools* de liquidez operados dentro de ambientes autorizados, com regras de participação, transparência e supervisão compatíveis com o regime vigente.

A experiência do Project Guardian, em Singapura, e do DLT Pilot Regime, na União Europeia, oferece indicações de como essa integração vem sendo testada em outras jurisdições.

5.4.Síntese

A proteção patrimonial e a gestão de garantias em ambiente tokenizado não dispensam a arquitetura regulatória existente, mas a reconfiguram. O livro-razão compartilhado pode eliminar reconciliações redundantes e tornar a verificação de posições mais direta. A segregação individual por endereço pode reforçar a proteção contra insolvência. Os contratos inteligentes podem automatizar fluxos de colateral.

Esses ganhos, porém, dependem de decisões de arquitetura, como a opção entre segregação individual e *omnibus*, a definição das regras codificadas no contrato inteligente e a governança sobre alterações no protocolo, que são, em última instância, decisões regulatórias, não tecnológicas.

6. Dados e interoperabilidade

A reconciliação periódica de posições entre os participantes da cadeia de pós-negociação é um dos pilares da integridade do mercado brasileiro.

Escrituradores, depositários centrais e custodiantes conciliam diariamente suas bases para assegurar correspondência entre titularidade plena, titularidade fiduciária e posições nas contas de custódia. Essa conciliação é eficaz, mas onerosa e existe porque cada participante opera um registro próprio, e a integridade do conjunto depende da conferência permanente entre registros independentes.

A promessa central da DLT para esse domínio é a substituição de múltiplas bases independentes por um livro-razão compartilhado, no qual as posições de todos os participantes sejam deriváveis de uma mesma fonte.

Se essa substituição se concretizar, a reconciliação periódica perde sua razão de ser, como mencionamos anteriormente. Não há o que conciliar quando todos leem o mesmo registro. A conciliação, que hoje é atividade recorrente e custosa, converte-se em verificação contínua e automatizada.

6.1.Risco de fragmentação

A interoperabilidade entre infraestruturas de mercado é um dos pontos em que a DLT pode complicar o cenário atual. Se múltiplas infraestruturas operam sobre a mesma rede ou sobre redes compatíveis, a troca de informações e a transferência de ativos entre elas tornam-se tecnicamente mais simples.

Contudo, se cada infraestrutura adota uma rede própria, com padrões distintos de representação de ativos, identificação de participantes e tratamento de eventos, a interoperabilidade exige pontes, padrões comuns de mensageria e acordos de governança, reproduzindo, em novo registro, os desafios que já existem entre os sistemas atuais.

A experiência internacional com pontes entre redes (*bridges*), como mencionado na seção 1, acumula histórico expressivo de incidentes de segurança, o que reforça a necessidade de tratar a interoperabilidade não apenas como problema técnico, mas como problema de desenho institucional[50].

Assim, o potencial do uso de DLT depende de condições que não se verificam automaticamente.

A primeira é que o livro-razão compartilhado seja aceito, pelas partes e pela regulação, como fonte autoritativa para fins de titularidade, movimentação e prova. Enquanto os participantes mantiverem bases paralelas por exigência regulatória, por precaução ou por necessidade operacional, a reconciliação não será eliminada; será duplicada.

A segunda condição é que a rede inclua todos os participantes relevantes da cadeia[51]. Se o escriturador opera fora da rede, ou se o sistema de liquidação financeira não está integrado, a conciliação entre o que está *on-chain* e o que está

[50] As pontes *cross-chain* (ferramentas que conectam diferentes redes blockchain) são consideradas um dos pontos mais fracos e vulneráveis da infraestrutura de criptomoedas, apresentando riscos de segurança severos que frequentemente resultam em perdas massivas. As pontes precisam conectar duas arquiteturas de blockchain totalmente diferentes, o que introduz uma camada extra e elevada de complexidade tecnológica. A operação depende de *smart contracts*, e pequenos erros de lógica ou bugs no código podem resultar na perda total de ativos ou em acessos não autorizados. As pontes exigem que os usuários bloqueiem seus ativos na rede de origem para cunhar a representação equivalente na rede de destino. Isso cria "potes de mel" (*honey pots*) com centenas de milhões de dólares agrupados em um único contrato, tornando-as alvos prioritários e extremamente lucrativos para hackers. Se as pontes carecerem de proteções criptográficas adequadas, atacantes podem interceptar uma transação válida e "repeti-la" inúmeras vezes para drenar os ativos bloqueados, ou explorar a ponte para realizar gastos duplos entre as diferentes cadeias. Cf. LEWIS, Rhian. *Understanding decentralized finance*: how DeFi is changing the future of money. London: Kogan Page, 2023. Cf. também ARMSTRONG, Ben. *Catching up to crypto*: your guide to Bitcoin and the new digital economy. Hoboken, NJ: Wiley, 2023.

[51] Uma proposta para evitar a fragmentação é a adoção de um modelo de Depositária "Soberana": Para contornar as restrições jurisdicionais, os autores propõem que cada mercado doméstico tenha o seu próprio registro distribuído "soberano", operando em uma blockchain permissionada (utilizando mecanismos de consenso como o PBFT - *Practical Byzantine Fault Tolerance*). A rede seria mantida por nós conhecidos (os próprios bancos, custodiantes e corretoras), garantindo que todos os valores mobiliários fiquem em um único registro nacional e evitando a fragmentação do mercado. Cf. EVERETT, Steve; CALITZ, Andre; GREYLING, Jean. The case for a 'sovereign' distributed securities depository for securities settlement. *Journal of Securities Operations & Custody*, Londres, v. 9, n. 3, p. 269-292, 2017.

fora da rede permanece necessária. O valor do blockchain depende do efeito de rede (quanto mais usuários, maior o benefício). Construir uma rede colaborativa do zero no setor financeiro e atrair uma massa crítica é imensamente difícil. Em vez de sistemas isolados em "silos", as IMFs podem garantir a interoperabilidade e a definição de padrões universais para o mercado de ativos digitais, assim como fazem hoje no mercado tradicional[52].

A terceira condição é que a governança da rede ofereça as mesmas garantias de integridade, disponibilidade e rastreabilidade que a regulação hoje exige de cada prestador isoladamente.

A quarta é a padronização. Se o mercado não conseguir superar a relutância em lidar com problemas de padronização do legado, é improvável que a DLT ofereça uma solução eficaz.

6.2.Portabilidade

A portabilidade é diretamente afetada pelas decisões de arquitetura. No modelo vigente, a transferência de posições entre custodiantes envolve comunicação entre os dois prestadores, verificação documental, instrução ao depositário central e atualização das contas em múltiplos sistemas.

A Resolução CVM nº 209/2024 estabeleceu prazo máximo de dois dias úteis para transferências com alteração de titularidade e introduziu regras de transparência sobre documentação necessária.

Em um ambiente tokenizado, a portabilidade pode ser simplificada pela movimentação direta dos ativos entre endereços na rede, desde que os mecanismos de identificação e compliance sejam preservados. A condição é que o novo custodiante esteja integrado à mesma rede ou que haja mecanismos de interoperabilidade confiáveis entre redes distintas.

[52] JIANG, Qian. Crossing the chasm: why post-trade FMIs are the key to scaling blockchain adoption. *Journal of Securities Operations & Custody*, v. 17, n. 2, p. 119-129, 2025. Disponível em: https://doi.org/10.69554/ANCK7901.

6.3.Informações aos investidores

A prestação de informações aos investidores é outro eixo do impacto da DLT sobre dados e transparência. No regime vigente, depositários centrais e custodiantes devem fornecer ao investidor informações sobre posição consolidada, movimentações e eventos, com periodicidade e meios padronizados. O escriturador tem deveres informacionais perante o emissor e perante investidores cujos valores mobiliários não estejam em depósito centralizado.

Em um ambiente tokenizado, o investidor pode, em princípio, consultar diretamente na rede o saldo de seus ativos, o histórico de movimentações e os gravames constituídos, sem depender exclusivamente do extrato fornecido pelo custodiante ou pelo escriturador.

Essa transparência direta não elimina, porém, a necessidade de informações organizadas e contextualizadas[53].

A consulta bruta à rede exige capacidade técnica que a maioria dos investidores de varejo não possui. Os dados *on-chain* podem não conter todas as informações relevantes para o investidor, como projeções de fluxo, cálculos de rendimento ou detalhes de eventos corporativos que dependam de decisões do emissor ainda não registradas na rede.

Assim, o papel do custodiante e do escriturador como organizadores e tradutores da informação tende a persistir, mesmo que a fonte primária dos dados migre para o livro-razão compartilhado.

Outra dimensão relevante da transparência diz respeito às informações sobre os criptoativos negociados, o que pode ocorrer sem divulgações

[53] HABIB, G.; et al. Blockchain Technology: Benefits, Challenges, Applications, and Integration. *Computers*, v. 14, n. 11, 2022. Disponível em: https://www.mdpi.com/1999-5903/14/11/341. O estudo destaca que o acesso direto a dados *on-chain* permite transparência, auditabilidade e verificação independente de transações sem intermediários, reduzindo assimetrias informacionais e dependência de *trusted third parties*, ao custo de expor usuários à complexidade técnica e à necessidade de interpretação adequada de dados brutos distribuídos.

adequadas sobre o ativo, seu emissor, riscos associados e histórico de operações. A ausência de padrões substanciais de listagem expõe investidores a assimetrias informacionais severas.

Adicionalmente, *exchanges* que listam e negociam ativos nos quais têm interesse material ou que emitiram diretamente enfrentam conflitos agudos de interesse, com potencial de uso de informação privilegiada e incentivo a promover negociação não adequada ao interesse do cliente.

A IOSCO preconiza[54] que os reguladores devem estabelecer, manter e divulgar publicamente padrões substantivos e procedimentais para admissão e exclusão de criptoativos à negociação, incluindo características do ativo, riscos, histórico de negociação, concentração de titularidade, protocolos de transferência e tratamento de eventos como *hard forks* e *airdrops*. Para stablecoins, exigências adicionais incluem divulgação sobre ativos de reserva, mecanismo de paridade, direitos de resgate e segregação patrimonial. Quanto aos conflitos em mercados primários, os reguladores devem avaliar se é necessário impor vedação à listagem ou facilitação de negociação de ativos nos quais as *exchanges* ou suas afiliadas detenham interesse material.

6.4.Rastreabilidade

A rastreabilidade de transações, por sua vez, é uma propriedade nativa de redes distribuídas. Cada transação registrada na rede é imutável, sequenciada e verificável por qualquer participante autorizado.

Essa propriedade oferece ganhos para os controles internos de prevenção à lavagem de dinheiro e a outras infrações de mercado. A trilha de auditoria, que no modelo atual é construída a partir de registros internos de cada

[54] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Policy Recommendations for Crypto and Digital Asset Markets*. Madrid, 2023. Disponível em https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf.

participante, pode ser complementada ou substituída por uma trilha derivável diretamente da rede, com menor risco de manipulação ou inconsistência.

Esse ganho, contudo, convive com uma tensão[55]. Em redes públicas ou semipúblicas, a rastreabilidade de transações pode entrar em conflito com obrigações de sigilo sobre posições e dados dos investidores, previstas nas três resoluções da CVM.

A pseudonimidade oferecida por endereços criptográficos não equivale a anonimato, e técnicas de análise *on-chain* permitem, com frequência, associar endereços a pessoas ou entidades. O desenho de privacidade da rede precisa equilibrar a rastreabilidade necessária para fins regulatórios e a proteção do sigilo exigida pela regulação[56].

Em redes permissionadas, esse equilíbrio é mais fácil de calibrar, porque o acesso à informação pode ser estratificado por perfil de participante. O regulador pode ter acesso integral ao histórico de transações, enquanto participantes comuns veem apenas as transações de que são parte.

Esse modelo, porém, reintroduz a necessidade de mecanismos de controle de acesso e governança de dados que, em redes públicas, são tratados pelo próprio protocolo.

---

[55] BELEN-SAGLAM, Rahime et al. A systematic literature review of the tension between the GDPR and public blockchain systems. *Blockchain: Research and Applications*, v. 4, n. 2, jun. 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S2096720923000040. Nesta revisão de literatura sobre o tema, são consolidadas evidências de que a rastreabilidade e a transparência ampliam a auditabilidade, mas colidem com princípios de minimização de dados e direito ao esquecimento, destacando dificuldades práticas na qualificação de agentes e na aplicação territorial das normas de proteção de dados.

[56] YAO, Qian. *Blockchain-based New Financial Infrastructures*: Theory, Practice and Regulation. Singapore: Springer, 2022. O autor aprofunda as soluções arquitetônicas delineadas para mitigar essa dicotomia, argumentando que a transparência e a rastreabilidade nativas da blockchain precisam ser submetidas a modelos operacionais de restrição de visibilidade (canais privados e arquiteturas *need-to-know*) ou primitivas criptográficas (criptografia homomórfica e assinaturas em anel), assegurando que a auditabilidade descentralizada dos fluxos de ativos não comprometa o rigoroso sigilo comercial intrínseco aos ecossistemas de infraestrutura financeira.

Adicionalmente, a visibilidade das transações pode intensificar corridas sobre criptoativos e funcionar como dispositivo de coordenação entre usuários, cujos incentivos a sacar aumentam quando observam movimentos semelhantes de outros participantes[57].

6.5.Dados *on-chain*, *off-chain* e oráculos

Um tema relevante é a definição do conteúdo adequado do livro-razão compartilhado. Registrar dados em uma rede distribuída implica custo de sincronização entre os nós participantes. Esse custo varia conforme o mecanismo de consenso, o tamanho dos blocos e o volume de transações, mas tende a ser significativamente superior ao custo de registrar dados em um banco de dados centralizado. Dados muito granulares, como históricos completos de movimentação, metadados de cada instrução ou detalhes de eventos corporativos em andamento, podem tornar o custo de operação da rede proibitivo[58].

A escolha sobre o que deve residir *on-chain* e o que deve permanecer *off-chain* é, por isso, uma das decisões de arquitetura de maior impacto[59]. O critério

[57] BASEL COMMITTEE ON BANKING SUPERVISION (BCBS). *Novel risks, mitigants and uncertainties with permissionless distributed ledger technologies*. Working Papers, n. 44. Basel, 2024. Disponível em https://www.bis.org/bcbs/publ/wp44.pdf.

[58] Se os blocos fossem muito grandes ou ilimitados, eles exigiriam um poder computacional, largura de banda e capacidade de armazenamento de dados muito maiores dos computadores que participam da rede (nós). Como resultado, computadores comuns não conseguiriam acompanhar o processamento, e apenas uma pequena quantidade de grandes corporações ou mineradores de escala industrial teriam recursos para manter nós completos, o que centralizaria a rede e destruiria o seu propósito original. Além disso, nlocos maiores levam muito mais tempo para serem transmitidos e propagados por toda a rede de computadores. Esse atraso aumenta a probabilidade de geração de blocos obsoletos (*stales*) ou órfãos, o que prejudica o consenso e reduz a segurança da blockchain. Por fim, Como todos os nós completos precisam baixar e armazenar todo o histórico da blockchain, blocos gigantescos fariam com que o tamanho total do *ledger* crescesse dezenas de terabytes rapidamente. Isso inviabilizaria que novos nós baixassem todo o histórico e mantivessem uma cópia da rede. Cf. BUTERIN, Vitalik. *Proof of stake*: the making of Ethereum and the philosophy of blockchains. New York: Seven Stories Press, 2022.

[59] GLOBAL FINANCIAL MARKETS ASSOCIATION. The impact of distributed ledger technology in capital markets. Washington: GFMA, 2025. Disponível em:

geral é que devem estar *on-chain* os dados cuja integridade, imutabilidade e verificabilidade por múltiplas partes constituam ganho funcional em relação ao modelo centralizado.

Tipicamente, esses dados envolvem saldos, registros de transferência, constituição e desconstituição de gravames e registros de liquidação. Dados auxiliares, como documentação de compliance, detalhes contratuais de cada operação, históricos de comunicação entre participantes e informações cadastrais, tendem a permanecer *off-chain*, consultados via oráculos e/ou armazenados em sistemas convencionais dos participantes, com referências criptográficas (*hashes*) registradas na rede para fins de verificação de integridade.

Esse modelo, frequentemente descrito como *on-chain*/*off-chain*, preserva os ganhos de transparência e verificabilidade para os dados estruturantes, sem onerar a rede com informações cuja granularidade não justifica o custo de sincronização[60].

A condição para que tal arranjo funcione é que os mecanismos de referência cruzada entre os dois ambientes sejam confiáveis e auditáveis. Se o *hash* registrado na rede garante que o documento *off-chain* não foi adulterado, mas o documento *off-chain* se torna inacessível, a referência perde utilidade prática.

Enquanto o armazenamento *off-chain* lida com dados estáticos ou documentos pesados, os oráculos lidam com o fluxo de informações dinâmicas

---

https://www.gfma.org/wp-content/uploads/2025/08/2.-exec-sum-impact-of-dlt-in-cap-mkts-final.pdf.

[60] COLLE, L. Reaching for the Moon: An Analysis of Real-Time Securities Clearing and Settlement in Light of Emerging Blockchain Technologies. *Virginia Law & Business Review*, v. 16, n. 3, p. 601-646, 2022. O autor corrobora a imperatividade de aliviar o volume transacional na cadeia principal (*on-chain*) por meio da adoção de protocolos de segunda camada (*layer-two protocols*), que viabilizam a consolidação e a compensação paralela (*netting*) de operações fora da rede (*off-chain*), enquanto os oráculos atuam como pontes informacionais operadas por terceiros para alimentar a blockchain (sistemicamente isolada) com os gatilhos de dados necessários à liquidação dos contratos.

do mundo real. Eles são servidores, entidades ou *smart contracts* específicos que atuam como um canal de comunicação, importando dados *off-chain* para dentro do ambiente *on-chain*[61].

Os *smart contracts* são códigos determinísticos que executam regras automaticamente, mas são isolados. Eles não conseguem acessar a internet ou julgar por si mesmos a veracidade de eventos que ocorrem fora da rede. Para que um *smart contract* financeiro execute uma liquidação, um derivativo ou uma chamada de margem, ele frequentemente precisa saber o preço atual de um ativo no mercado tradicional, uma taxa de câmbio ou até mesmo a temperatura de uma cidade. Nesse cenário, o oráculo é o agente responsável por coletar essas informações externas, validá-las e inseri-las na blockchain.

A conexão do mundo *on-chain* impecável com o mundo *off-chain* inerentemente imperfeito gera um desafio crítico conhecido como o "problema do oráculo" – como fazer com que o mensageiro não comprometa a mensagem? Se um oráculo transmitir dados falsos, atrasados ou for alvo de hackers, o *smart contract* executará a ação de forma incorreta (e irreversível), o que já causou perdas de centenas de milhões de dólares no mercado[62].

Para que o arranjo híbrido funcione de maneira confiável, as plataformas exigem a diversificação de múltiplas fontes de oráculos, auditorias e protocolos de segurança rigorosos, ou a utilização de oráculos descentralizados e ambientes de execução confiáveis para mitigar o risco de manipulação da informação do mundo real.

---

[61] DULEY, Chanelle et al. *The oracle problem and the future of DeFi*. BIS Bulletin, n. 76. Basel, 2023. Disponível em: https://www.bis.org/publ/bisbull76.pdf.

[62] DI MAGGIO, Marco. Blockchain, crypto and DeFi: bridging finance and technology. 1. ed. Hoboken, NJ: Wiley, 2024. O autor enuncia o problema como "*the turst conumdrum*".

6.6.Cadastro de usuários

O impacto sobre o cadastro de usuários segue lógica semelhante. As obrigações de identificação do investidor, previstas na Resolução CVM nº 50/2021 e na regulação de prevenção à lavagem de dinheiro, exigem coleta, verificação e atualização de dados pessoais, com trilha de auditoria e acesso imediato aos registros.

Soluções de identidade descentralizada (*decentralized identity* - DID), identidade soberana (*self-sovereign Identity* - SSID) ou de credenciais verificáveis (*verifiable credentials*)[63] podem simplificar o processo de *onboarding*, permitindo que o investidor comprove sua identidade uma única vez e reutilize a credencial perante múltiplos prestadores.

O cadastro em si, contudo, não precisa residir integralmente na rede. A credencial verificável pode ser emitida *off-chain* e referenciada *on-chain* para fins de controle de acesso, preservando a privacidade dos dados pessoais e reduzindo o custo de armazenamento na rede[64].

---

[63] BRUNNER, Clemens et al. DID and VC: untangling decentralized identifiers and verifiable credentials for the Web of Trust. In: *Proceedings of the 3rd International Conference on Blockchain Technology and Applications, Xi'an, China, 14-16 dez. 2020*. New York: ACM, 2020. Disponível em https://doi.org/10.1145/3446983.3446992. O trabalho sistematiza a arquitetura de identidade descentralizada baseada em blockchain, distinguindo claramente três papéis – *issuer*, *holder* e *verifier* – e demonstrando que *verifiable credentials* funcionam como declarações criptograficamente assinadas que podem ser verificadas independentemente do emissor original, reduzindo a dependência de autoridades centrais e permitindo modelos de confiança distribuída. Cf. também SCHARDONG, Frederico; CUSTÓDIO, Ricardo. Self-sovereign identity: a systematic review, mapping and taxonomy. *Sensors*, v. 22, n. 15, 2022. Disponível em: https://doi.org/10.3390/s22155641. A revisão evidencia que a self-sovereign identity representa uma mudança de paradigma ao conferir ao usuário controle sobre coleta, armazenamento e compartilhamento de dados pessoais, sendo operacionalizada por DIDs e VCs que viabilizam divulgação seletiva e minimização de dados, com impactos diretos sobre privacidade e governança.

[64] CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE (CCAF). *Digital Public Infrastructure and Digital Financial Services*: Convergence, Landscape and Regulatory Considerations. Cambridge, 2025. Disponível em https://www.jbs.cam.ac.uk/2025/global-regulatory-trends-for-digital-public-infrastructure/. O relatório contrapõe a eficiência dos modelos de identidade centralizados aos arranjos descentralizados autosssoberanos (SSID), constatando que estes últimos, conquanto efetivamente empoderem os indivíduos e maximizem a proteção da

Essa arquitetura altera a lógica tradicional de KYC[65]. Em vez de um modelo baseado na coleta redundante e armazenamento massivo de dados por múltiplos intermediários, o uso de DLT associado a credenciais verificáveis permite a constituição de um ecossistema de confiança distribuída, no qual emissores, titulares e verificadores operam em um arranjo triangular.

Nesse modelo, entidades confiáveis emitem atestações assinadas criptograficamente, o investidor as mantém sob sua custódia e as apresenta quando necessário, cabendo ao verificador apenas confirmar sua autenticidade e integridade, sem necessidade de acesso à base completa de dados subjacente.

Assim, o foco desloca-se para a confiabilidade do emissor, a robustez do processo de identificação original e o estado da credencial – validade, integridade e eventual revogação.

Com isso, torna-se viável a portabilidade de KYC. Credenciais podem ser reutilizadas entre instituições, reduzindo custos, redundâncias e fricções no onboarding. Ao mesmo tempo, o modelo tende a diminuir a sobrecoleta de dados, ao permitir que apenas atributos específicos sejam compartilhados, conforme a finalidade da operação.

A identificação do beneficiário final também pode ser reconfigurada. Em vez de depender exclusivamente de cadeias documentais fragmentadas, é possível estruturar camadas de credenciais emitidas por diferentes atores. Essas atestações, quando combinadas, permitem reconstruir a titularidade econômica com maior consistência e auditabilidade.

Há, contudo, limites relevantes. O modelo não elimina a necessidade de avaliação de risco contextual exigida pela regulação de PLD/FT. A dependência

---

privacidade na interação com infraestruturas públicas digitais, impõem desafios sistêmicos complexos de governança e de responsabilização (*accountability*) sob a perspectiva regulatória.

[65] WORLD ECONOMIC FORUM. *Reimagining Digital ID*. Geneva, 2023. Disponível em: https://www.weforum.org/publications/reimagining-digital-id/. O relatório descreve o modelo de *trust triangle* entre emissores, titulares e verificadores, que fundamenta a substituição da coleta direta de dados por verificação de credenciais.

de emissores confiáveis cria novos pontos críticos. Além disso, riscos de correlação de dados e rastreabilidade persistem, especialmente se identificadores forem reutilizados entre contextos distintos.

Portanto, o uso de DLT não reduz o rigor das obrigações de identificação, mas transforma sua implementação. A ênfase desloca-se da custódia de dados para a verificação de credenciais e para a gestão de confiança entre participantes, com ganhos potenciais de eficiência, mas também novos desafios regulatórios e operacionais.

6.7.Síntese

O compartilhamento de dados entre infraestruturas é, em última instância, o problema que a interoperabilidade técnica pretende resolver, mas que só se resolve de fato quando acompanhado de acordos de governança, padronização de formatos e definição clara de responsabilidades pelo tratamento das informações compartilhadas.

A DLT pode facilitar o compartilhamento ao oferecer uma base de dados comum, mas a decisão sobre quem acessa o quê, em que condições e com que finalidade permanece institucional, não tecnológica.

Pelo exposto, o uso de DLT pode alterar substancialmente os fluxos de dados e os processos de reconciliação da cadeia de pós-negociação, com ganhos de eficiência, rastreabilidade e transparência.

Esses ganhos, porém, são condicionados a escolhas de desenho que envolvem o conteúdo do livro-razão, a arquitetura de privacidade, a integração entre ambientes *on-chain* e *off-chain* e a definição de qual participante ou autoridade tem acesso a cada camada de informação.

7. Desafios e riscos

A utilização de DLT em infraestruturas de mercado financeiro não apenas redistribui funções entre participantes. Ela altera a matriz de riscos e

introduz problemas de governança que não encontram equivalente direto no modelo vigente. A avaliação desses desafios exige distinguir quatro planos, que são a governança da rede, os riscos operacionais, cibernéticos e tecnológicos, as concessões estruturais impostas pelo chamado trilema da DLT e os impedimentos ao desenvolvimento de mercado que condicionam a viabilidade econômica e jurídica de qualquer iniciativa de tokenização em escala.

7.1.Governança

No modelo atual, a governança das infraestruturas é exercida por entidades juridicamente identificáveis, com órgãos estatutários, regulamentos aprovados pela CVM, diretores responsáveis, estrutura de autorregulação e mecanismos de supervisão e sanção. As decisões sobre mudanças nos sistemas, critérios de participação, regras de movimentação e tratamento de incidentes seguem processos formais, sujeitos a aprovação prévia do regulador quando materialmente relevantes. A responsabilidade institucional é clara.

A introdução de DLT tensiona esse modelo em vários pontos[66].

O primeiro é a definição de quem decide sobre a arquitetura da rede. Em redes permissionadas voltadas a infraestruturas reguladas, essa decisão tende a recair sobre um consórcio de participantes ou sobre uma entidade operadora designada. A escolha do mecanismo de consenso, da política de validação, dos padrões de interoperabilidade e das regras de admissão e exclusão de nós são,

[66] PAECH, Philipp. The governance of blockchain financial networks. *Modern Law Review*, v. 80, n. 6, p. 1073–1110, 2017. Disponível em https://doi.org/10.1111/1468-2230.12303. O autor enquadra a rede blockchain financeira como arranjo de governança e não como mera arquitetura computacional, o que é especialmente relevante em blockchains permissionadas para infraestrutura de mercado, nas quais entrada, validação, atualização do protocolo, alocação de responsabilidades e resolução de conflitos dependem de escolhas jurídicas e institucionais ex ante. Seu argumento é que, para ativos financeiros, o problema decisivo não é apenas registrar posições, mas estruturar fronteiras entre regulação financeira, direito privado e regras internas da rede, pois é essa combinação que transforma incentivos tecnológicos dispersos em obrigações estáveis, oponíveis e compatíveis com proteção de participantes e estabilidade sistêmica

todas elas, decisões com impacto direto sobre segurança, desempenho e equidade de acesso.

Se essas decisões forem tomadas por maioria de participantes sem supervisão externa, há risco de captura por atores dominantes. Se forem centralizadas em um único operador[67], reproduz-se a estrutura tradicional, com o custo adicional de uma camada tecnológica que não gera os benefícios esperados da distribuição.

Os atuais Depositários Centrais (CSDs) são vistos como os candidatos mais aptos a reter o papel de "policiamento" e governança, atuando como guardiões de confiança (*trusted gatekeepers*) para autorizar o acesso à rede, administrar participantes e gerir eventuais processos de insolvência[68].

Nesse contexto se insere também a gestão de mudanças no protocolo. Atualizações de software, correção de vulnerabilidades, alteração de parâmetros de consenso e migração de versões exigem coordenação entre todos os nós da rede. Em redes públicas, esse processo é frequentemente conflituoso, podendo resultar em *forks* que fragmentam a base de participantes e criam versões concorrentes do mesmo registro[69]. Em redes permissionadas, a coordenação é mais controlável, mas ainda exige governança formal para

[67] Um exemplo notório é a plataforma D-FMI da Euroclear, onde o próprio Euroclear Bank atua como o único operador da rede (sole network operator), mantendo o controle estrutural para garantir a conformidade com regulações rigorosas e com os PFMI. D-FMI (Digital Financial Market Infrastructure) da Euroclear, é uma plataforma baseada em DLT para emissão, distribuição e liquidação de Digitally Native Notes (DNNs), com integração ao sistema tradicional para liquidação secundária.

[68] MEIJER, Carlo R. W. de. The roles of CSDs in a blockchain environment. *Journal of Securities Operations & Custody*, v. 12, n. 2, p. 167-174, 2020.

[69] Em certas redes DLT, discordâncias na governança ou a necessidade de atualizações podem levar a um *fork* (bifurcação da rede), dividindo o blockchain em dois. Isso pode causar sérios problemas operacionais, atrasos na implementação de correções de segurança e incertezas sobre qual cadeia de blocos representa a versão legítima da propriedade do ativo. Cf. FINANCIAL STABILITY BOARD (FSB). *The Financial Stability Implications of Tokenisation*. Basel, 2024. Disponível em: https://www.fsb.org/uploads/P221024-2.pdf.

definir quem propõe, quem aprova e quem implementa as alterações, além de mecanismos de reversão em caso de falha.

Outro ponto relevante é a gestão de incentivos[70]. Em redes públicas, os validadores são remunerados pelo protocolo, o que alinha seus incentivos à manutenção da rede, mas não necessariamente ao cumprimento de obrigações regulatórias.

Em redes permissionadas voltadas a infraestruturas de mercado, os validadores tendem a ser os próprios participantes regulados, cujos incentivos já são disciplinados pela regulação.

A questão que se coloca é como conciliar a estrutura de incentivos da rede com as obrigações fiduciárias, de conduta e de supervisão que recaem sobre cada participante individualmente, e como tratar situações em que o interesse econômico do validador na rede conflita com seus deveres perante clientes ou perante o regulador.

O risco de fragmentação de mercado perpassa todos esses pontos (ver seção 6.1). Se diferentes infraestruturas adotarem redes distintas, com padrões incompatíveis de representação de ativos, identificação de participantes e tratamento de eventos, o resultado será a criação de ilhas ou silos de ativos tokenizados.

Ativos emitidos em uma rede não serão facilmente negociáveis em outra. A liquidez se fragmentará. A interoperabilidade exigirá pontes com custos e riscos próprios. A experiência da internet sugere que a adoção em larga escala

[70] AUER, Raphael; MONNET, Cyril; SHIN, Hyun Song. *Permissioned distributed ledgers and the governance of money*. BIS Working Papers, Basel, n. 924, jan. 2021. Disponível em https://www.bis.org/publ/work924.htm. Os autores oferecem, talvez, a formulação econômica mais direta do problema dos incentivos em DLT permissionada: validadores conhecidos incorrem em custos de verificação e comunicação, não podem ser compelidos tecnicamente a verificar cada operação e podem, em tese, aceitar subornos para validar históricos falsos; por isso, a integridade do *ledger* depende de um desenho institucional que combine remuneração suficiente, número ótimo de validadores, regra de supermaioria e dimensão das transações. O ponto central é que maior robustez do consenso exige rendas maiores para os validadores, de modo que a descentralização permissionada não é gratuita

de infraestruturas distribuídas depende de padronização, protocolos abertos e construção de uma rede de redes.

No mercado de capitais, essa padronização não pode ser deixada ao jogo espontâneo dos participantes. Ela exige coordenação regulatória, definição de padrões mínimos de interoperabilidade e, possivelmente, designação de camadas comuns de infraestrutura sobre as quais os diferentes participantes possam operar.

7.2.Riscos operacionais, cibernéticos e tecnológicos

Os riscos associados ao uso de DLT em infraestruturas de mercado não são inteiramente novos. Risco operacional, risco cibernético e risco tecnológico já são objeto de tratamento nas resoluções CVM 31, 32 e 33, que exigem sistemas seguros e adequados, planos de contingência, duplicação de informações, controles de acesso, rastreabilidade e comunicação de incidentes. A diferença está na forma como esses riscos se manifestam em ambiente distribuído e nos mitigadores que esse ambiente exige[71].

O *risco operacional* em infraestruturas baseadas em DLT diz respeito a perdas resultantes de inadequações ou falhas em processos internos, sistemas, pessoas ou eventos externos, com especial relevância, a perda de chaves criptográficas[72]. Conforme já indicado na seção sobre custódia, a perda (ou o furto ou má gestão) de uma chave pode significar a perda irreversível do ativo,

[71] FINANCIAL STABILITY BOARD (FSB). *The Financial Stability Implications of Tokenisation*. Basel, 2024. Disponível em: https://www.fsb.org/uploads/P221024-2.pdf. O FSB identifica cinco categorias de vulnerabilidades associadas à tokenização baseada em DLT, incluindo fragilidades operacionais, riscos de interconexão e alavancagem. Ainda, registra que os riscos operacionais da transição para DLT incluem a potencial instabilidade de redes quando utilizadas em escala e o maior potencial de ataques cibernéticos em comparação com infraestruturas tradicionais.

[72] BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *Financial stability risks from cryptoassets in emerging market economies*. BIS Papers, n. 138. Basel: BIS, ago. 2023. Disponível em: https://www.bis.org/publ/bppdf/bispap138.pdf.

sem possibilidade de recuperação por instância externa[73]. Esse risco não tem paralelo direto na infraestrutura tradicional, em que registros podem ser reconstruídos pela conciliação entre bases.

A exigência de operações contínuas (24/7) aumenta a pressão operacional e dificulta a realização de manutenções e atualizações de sistemas sem causar interrupções.

A segregação de funções, com separação entre quem gera, quem armazena e quem autoriza o uso das chaves, é o mitigador primário[74]. Mecanismos de assinatura múltipla, computação multipartidária e fragmentação de chaves (*key sharding*) distribuem o risco entre vários agentes, reduzindo a probabilidade de perda ou comprometimento por falha isolada. Procedimentos de backup e recuperação, com armazenamento em ambientes fisicamente distintos e sujeitos a controles de acesso rigorosos, complementam a proteção[75].

O *risco cibernético* assume contornos específicos em redes distribuídas. A superfície de ataque se amplia para incluir nós validadores, contratos inteligentes, oráculos e pontes entre redes, além dos vetores tradicionais de

[73] BANK FOR INTERNATIONAL SETTLEMENTS (BIS). COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES (CPMI). *Tokenisation in the context of money and other assets: concepts and implications for central banks*. CPMI Papers, n. 225. Basel: BIS, 21 out. 2024. Disponível em: https://www.bis.org/cpmi/publ/d225.pdf.

[74] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Policy Recommendations for Crypto and Digital Asset Markets*. Madrid, 2023. Disponível em https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf. Os provedores de serviços de criptoativos (*crypto-asset service providers*, CASPs) frequentemente concentram, sob uma mesma entidade jurídica ou grupo, funções que em mercados tradicionais são segregadas: operação de ambiente de negociação, corretagem, formação de mercado, negociação proprietária, custódia, compensação e liquidação, além de serviços de empréstimo e staking. Essa integração vertical cria conflitos estruturais cujos efeitos se potencializam quando o investidor de varejo não compreende em que capacidade o CASP está atuando. De acordo com a IOSCO, a regulação deve exigir que os CASPs adotem governança e arranjos organizacionais efetivos, com sistemas, políticas e procedimentos para identificar, gerenciar e mitigar conflitos.

[75] COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES (CPMI); BOARD OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Guidance on cyber resilience for financial market infrastructures*. CPMI Papers, n. 146. Basel, 2016. Disponível em: https://www.bis.org/cpmi/publ/d146.pdf.

ataque a sistemas centralizados. A engenharia social dirigida a operadores de nós ou a detentores de chaves administrativas pode comprometer a integridade de toda a rede. *Insider threats*, isto é, ameaças originadas por pessoas com acesso legítimo aos sistemas, ganham gravidade adicional quando o acesso permite assinar transações irreversíveis.

Os mitigadores incluem controles de acesso estratificados, autenticação multifator, monitoramento contínuo de comportamento anômalo, simulações periódicas de ataque e políticas de resposta a incidentes com procedimentos de contenção e comunicação às autoridades e aos participantes afetados.

O *risco tecnológico* abrange vulnerabilidades nos protocolos da rede, vulnerabilidades em contratos inteligentes e eventos disruptivos como *forks*. Deriva especificamente da arquitetura da infraestrutura DLT e da programação dos softwares que sustentam a rede. Trata-se do risco da tecnologia falhar em seu funcionamento planejado[76].

Contratos inteligentes são, por natureza, difíceis de corrigir após a implantação, porque a imutabilidade é uma das propriedades que lhes confere confiabilidade. Essa mesma propriedade faz com que um erro no código possa ser explorado repetidamente até que uma intervenção extraordinária o corrija, com custos reputacionais e patrimoniais potencialmente elevados.

Auditorias periódicas de código, verificação formal de contratos inteligentes, programas de recompensa por identificação de vulnerabilidades (*bug bounties*) e mecanismos de pausa ou *circuit breaker* codificados no próprio contrato são mitigadores que a experiência do ecossistema de finanças descentralizadas consolidou, e cuja adoção em infraestruturas reguladas é condição mínima de operação segura[77].

---

[76] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Tokenization of financial assets*. Final Report FR17/2025. Madrid, 2025. Disponível em: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD809.pdf.

[77] O BCBS recomenda auditorias independentes e regulares do código-fonte de *smart contracts* e protocolos DLT *permissionless*, dado que a governança descentralizada dificulta a identificação e

A governança de aprovação e execução de transações opera como mitigador transversal. Em arranjos bem desenhados, nenhuma transação relevante é executada por decisão unilateral de um único agente. A aprovação depende de quórum, a execução é condicionada à verificação automatizada de regras de compliance, e o registro de cada etapa é imutável e auditável.

Essa arquitetura reproduz, em novo registro técnico, os princípios de controles internos e segregação de atividades que as resoluções da CVM já impõem aos prestadores de serviços de infraestrutura.

A continuidade de negócios em infraestruturas distribuídas apresenta nuances próprias. A distribuição de nós reduz o risco de ponto único de falha (*single point of failure*), mas se a rede depende de um número mínimo de validadores para atingir consenso, a indisponibilidade simultânea de validadores suficientes pode paralisá-la[78].

Os planos de continuidade precisam contemplar cenários de indisponibilidade de nós, comprometimento de chaves administrativas, bifurcação não planejada e migração de emergência. Uma métrica essencial para infraestruturas do mercado financeiro é possuir a capacidade de retomar as operações críticas dentro de um prazo máximo de duas horas (2hRTO) após o incidente, concluindo a liquidação das transações no mesmo dia, salvaguardando a estabilidade financeira[79].

---

correção de vulnerabilidades, aumentando o risco de perdas associadas a *bugs* ou *exploits*. Cf. BASEL COMMITTEE ON BANKING SUPERVISION (BCBS). *Novel risks, mitigants and uncertainties with permissionless distributed ledger technologies*. Working Papers, n. 44. Basel, 2024. Disponível em https://www.bis.org/bcbs/publ/wp44.pdf.

[78] A integração de múltiplas funções (negociação, emissão, liquidação e custódia) em um único intermediário ou plataforma DLT pode facilitar a rápida propagação de choques (contágio) para o sistema financeiro tradicional. Cf. FINANCIAL STABILITY BOARD (FSB). *The financial stability implications of multifunction crypto-asset intermediaries*. Basel, 2023. Disponível em: https://www.fsb.org/uploads/P281123.pdf.

[79] COMMITTEE ON PAYMENTS AND MARKET INFRASTRUCTURES (CPMI); BOARD OF THE INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Guidance on cyber resilience for financial market infrastructures*. CPMI Papers, n. 146. Basel, 2016. Disponível em: https://www.bis.org/cpmi/publ/d146.pdf.

As exigências já previstas para o depositário central, como ambiente de contingência em espaço físico distinto, podem ser adaptadas, mas não dispensadas.

De um lado, o uso de DLT elimina ou atenua certos riscos, como inconsistência entre bases de dados e ponto único de falha. De outro, introduz riscos que não existiam ou eram marginais, como perda irreversível de chaves, exploração de vulnerabilidades em contratos inteligentes e fragmentação de mercado. A regulação precisa avaliar cada configuração concreta à luz dos riscos que ela gera e dos mitigadores que efetivamente implementa.

7.3.Trilema e concessões estruturais

O chamado trilema da DLT postula que redes distribuídas enfrentam concessões estruturais entre três propriedades desejáveis, que são *descentralização*, *segurança* e *escalabilidade*. Não é possível maximizar as três simultaneamente com a tecnologia disponível[80].

Redes altamente descentralizadas e seguras tendem a processar poucas transações por segundo. Redes escaláveis e seguras tendem a concentrar a validação em poucos nós. Redes descentralizadas e escaláveis tendem a sacrificar garantias de segurança ou finalidade.

Para infraestruturas de mercado reguladas, esse trilema impõe escolhas claras. A segurança e a finalidade da liquidação são requisitos inegociáveis, conforme discutido na seção 2.2. A escalabilidade é necessária para processar o volume de operações dos mercados de capitais. A descentralização, embora desejável como mecanismo de resiliência e de redução de concentração, é o

[80] DYLAN-ENNIS, Paul. *Absolute Essentials of Ethereum*. Abingdon: Routledge, 2024. A obra atribui a formulação conceitual do trilema a Vitalik Buterin, parametrizando as três métricas fundamentais envolvidas na compensação: escalabilidade (transações por segundo), descentralização (quantidade de nós validadores) e segurança (resistência contra-ataques), ressaltando que a resposta técnica do ecossistema Ethereum a esse gargalo tem se concentrado na transição para soluções de Camada 2 (Layer 2).

vértice mais frequentemente sacrificado nas implementações voltadas a mercados regulados.

Por essa razão, a maioria das iniciativas internacionais adota redes permissionadas com número limitado de validadores, priorizando desempenho e finalidade determinística em detrimento da descentralização plena.

A consequência regulatória é que a DLT aplicada a infraestruturas de mercado tende a não ser "distribuída" no sentido forte do termo. Ela opera como base de dados compartilhada com propriedades de imutabilidade, rastreabilidade e automação por contratos inteligentes, governada por um conjunto restrito de participantes identificados e supervisionados. Tal configuração preserva ganhos tecnológicos reais, sobretudo na automação de fluxos e na eliminação de reconciliações, mas não produz a desintermediação radical que a narrativa mais entusiasmada da DLT promete.

7.4.Impedimentos ao desenvolvimento de mercado

A análise dos riscos técnicos e de governança em infraestruturas baseadas em DLT é incompleta sem considerar entraves econômicos, jurídicos e ecossistêmicos que dificultam a passagem de pilotos para operações viáveis. A OCDE, em 2025, sistematizou esses impedimentos com base em evidências comparadas, oferecendo um quadro que complementa a análise regulatória e tecnológica[81].

O primeiro problema é circular. A ausência de liquidez afasta emissores e investidores, o que impede a formação de um ecossistema mínimo. A superação desse ciclo exige um catalisador que concentre atividade, como emissões soberanas em DLT, e a digitalização coordenada de todo o ciclo do

[81] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Tokenisation of assets and distributed ledger technologies in financial markets*: potential impediments to market development and policy implications. Business and Finance Policy Paper, n. 75. Paris, 2025. Disponível em: https://doi.org/10.1787/40e7f217-en.

ativo. Quando processos seguem duplicados *on-chain* e *off-chain*, as eficiências não se concretizam.

O segundo obstáculo é econômico. Os benefícios dependem de escala e de efeitos de rede que não aparecem em projetos-piloto. Nesses contextos, os custos superam os ganhos observáveis. A decisão de migração requer evidência de eficiência. Soma-se a isso o fato de que parte dos benefícios atribuídos à tokenização já pode ser obtida por instrumentos tradicionais, o que reduz a urgência da adoção.

O terceiro entrave envolve a questão de entrega contra pagamento. A liquidação DvP integralmente *on-chain* pressupõe moeda tokenizada. Opções privadas carregam risco de crédito e liquidez e tensionam o princípio de unicidade da moeda. As CBDCs de atacado seguem em fase experimental.

O quarto obstáculo é operacional. A liquidação atômica elimina risco de principal, mas, quando instantânea, restringe a compensação, exige pré-financiamento (*pre-funding*) e eleva a demanda por liquidez intradiária. A programabilidade permite sincronizar entrega e pagamento sem instantaneidade, reproduzindo lógicas de DvP 2 e 3. A questão passa a ser o desenho de janelas de liquidação compatíveis com o pós-negociação.

O quinto entrave está na custódia. Custodiantes são a porta de entrada institucional e garantem a correspondência entre o token e o ativo subjacente. Sem essa verificação, a representação perde lastro. Embora haja avanço na oferta de serviços para ativos digitais, a integração de investidores a plataformas DLT com ativos regulados ainda é incipiente.

O sexto problema é a fragmentação. Redes permissionadas mitigam riscos de PLD/FTP, mas criam ilhas de liquidez. A interoperabilidade exige pontes ou padrões comuns, ambos com custos e riscos. Redes públicas ampliam escala, mas dificultam controle de acesso e execução de comandos regulatórios.

A sétima dificuldade é a ausência de padrões de identificação e dados. A falta de identificadores globais, normas de mensageria e regras contábeis claras

limita a integração e gera incerteza sobre classificação e registro. Padrões também viabilizam verificações automáticas de elegibilidade, reduzindo fricções operacionais. A padronização depende de coordenação regulatória.

O oitavo problema é jurídico. A titularidade do token nem sempre coincide com a titularidade do ativo. A executabilidade de *smart contracts* e a definitividade da liquidação variam entre jurisdições. Em operações transfronteiriças, essas divergências se ampliam. No Brasil, regimes de escrituração e depósito central conferem segurança à titularidade, mas a articulação com registros em DLT e a definição de qual ato produz efeito jurídico ainda demandam enfrentamento normativo.

Esse conjunto de obstáculos mostra que a maioria dos limites não é estritamente regulatória. Ainda assim, o desenho normativo influencia sua superação ao habilitar pagamentos *on-chain*, definir deveres de custódia, exigir padrões e conferir segurança jurídica. Sem ação coordenada, o potencial de eficiência e acesso da tokenização tende a não se materializar no mercado de capitais.

8. Arquiteturas possíveis

A passagem da análise de funcionalidades e riscos para a discussão de arquiteturas exige, antes de tudo, uma distinção funcional que o debate frequentemente obscurece.

A custódia de ativos virtuais, tal como disciplinada pela regulação de prestadores de serviços de ativos virtuais, envolve a guarda de criptoativos nativos, cuja existência se esgota na rede.

A custódia de valores mobiliários, regulada pela RCVM 32/21, envolve a guarda de ativos cuja existência jurídica é constituída por ato de emissão e escrituração, com efeitos perante terceiros e tratamento de eventos corporativos definidos pela regulação societária e do mercado de capitais.

A função de depositário central, regulada pela RCVM 31/21, vai além da guarda e abrange o controle centralizado de titularidade fiduciária, a disciplina da movimentação, a supervisão de participantes e a integração com sistemas de compensação e liquidação.

Essas três funções podem, em ambiente tokenizado, aproximar-se operacionalmente, mas não são equivalentes do ponto de vista jurídico e regulatório. A guarda de uma chave criptográfica que controla um token representativo de debênture não é a mesma atividade que a custódia de uma debênture escritural sob o regime da RCVM 32/21, nem equivale ao controle de titularidade fiduciária exercido pelo depositário central sob a RCVM 31/21. A regulação precisa manter essas distinções, mesmo que a tecnologia subjacente aproxime as operações.

8.1.Reposicionamento dos atores

A tokenização de valores mobiliários não elimina as funções desempenhadas pelos intermediários tradicionais, mas redistribui parte delas e altera os fluxos entre eles[82].

O custodiante, no ambiente tokenizado, desloca seu centro de gravidade da guarda de posições em conta para a guarda de chaves criptográficas[83]. A função de conservar, controlar e conciliar posições permanece, mas o objeto sob

[82] Um monopólio regulamentado (como as CSDs) continuará sendo vital para garantir a integridade das emissões de valores mobiliários e evitar a criação indevida de títulos, assegurando que o registrado na DLT corresponda à emissão real. A função de compensação (clearing) continuará sendo necessária para transações com derivativos que demandam a mitigação de risco de contraparte ao longo da vida do contrato. Cf. PINNA, Andrea; RUTTENBERG, Wiebe. *Distributed ledger technologies in securities post-trading*: revolution or evolution? Frankfurt am Main: European Central Bank, 2016. Disponível em https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf.

[83] IGNATOWICZ, Radoslaw; TAUDES, Alfred. Opportunities in digital assets and digital custody: tracking the modernisation of standard custody offering. *Journal of Securities Operations & Custody*, v. 15, n. 3, p. 194-204, 2023.

guarda é diferente, e os riscos associados são distintos, conforme analisado na seção 2.1.

A validação e autorização de transações, que no modelo atual é uma das atribuições operacionais do custodiante, torna-se inseparável da gestão das chaves, porque assinar uma transação na rede é o ato que efetiva a movimentação.

O escriturador, que no modelo vigente mantém os registros originários de titularidade, pode assumir em ambiente tokenizado a função de oráculo, isto é, a entidade que atesta, perante a rede, a correspondência entre o token e o ativo subjacente, a ocorrência de eventos corporativos, o cálculo de proventos e outras informações que o contrato inteligente precisa receber de fonte externa para executar seus fluxos. Essa função preserva o núcleo da atividade de escrituração, que é a produção de registros com fé pública ou efeito constitutivo, mas a reformula em termos de alimentação de dados para a rede.

O depositário central enfrenta o desafio mais complexo. Se o livro-razão distribuído passa a ser a fonte autoritativa de titularidade, a função de controle centralizado de titularidade fiduciária pode ser parcialmente absorvida pela rede.

A supervisão de participantes, a disciplina de movimentação e a integração com compensação e liquidação, porém, continuam exigindo uma entidade com poderes regulamentares, capacidade de inspeção e responsabilidade institucional.

O depositário central pode migrar de operador de um sistema proprietário de registros para operador ou co-governante de uma rede distribuída, sem que isso elimine sua função institucional[84].

[84] BAUVARS, J. Applicability of Blockchain Technology in Securities Settlement. *Complex Systems Informatics and Modeling Quarterly*, n. 28, p. 34-58, 2021. O autor propõe que, na transição para infraestruturas baseadas em tecnologia de registro distribuído (DLT), os depositários centrais de valores mobiliários (CSDs) assumam o papel de gestores da rede, definindo regras operacionais e exercendo funções de governança e supervisão estrita. Nesse modelo, a

As entidades administradoras de mercados organizados, que hoje operam ambientes de negociação com regras próprias de acesso, formação de preços, autorregulação e supervisão, precisam definir como essas funções se exercem quando a negociação ocorre em ambiente distribuído.

A autorregulação, em particular, depende de capacidade de monitoramento, instauração de processos disciplinares e imposição de penalidades, atribuições que pressupõem autoridade sobre os participantes e acesso aos registros de negociação. Em redes permissionadas, essas funções podem ser preservadas. Em redes públicas ou semipúblicas, a capacidade de supervisão é estruturalmente limitada.

As corretoras e distribuidoras, na qualidade de intermediários entre o investidor e o mercado, podem ter parte de suas funções simplificada pela negociação direta em rede, especialmente em mercados de balcão.

O dever de melhor execução, a identificação do comitente final, o controle de ordens e a prevenção de práticas não equitativas, contudo, não se automatizam pela simples adoção de DLT[85]. O intermediário continua sendo o

validação do estado da rede e da liquidação dos ativos é gerida pelo CSD, que atua validando os participantes e administrando as chaves criptográficas, dispensando mecanismos de consenso abertos e anônimos para compatibilizar a arquitetura com os rigorosos requisitos regulatórios do mercado.

[85] INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Policy Recommendations for Crypto and Digital Asset Markets*. Madrid, 2023. Disponível em https://www.iosco.org/library/pubdocs/pdf/IOSCOPD747.pdf. Clientes frequentemente ignoram que o CASP (Crypto Asset Service Provider) pode estar negociando contra eles, antecipando ordens (front-running) ou deixando de oferecer o melhor preço ou execução. A ausência de requisitos equivalentes aos dos mercados tradicionais em termos de transparência pré e pós-negociação cria mercados opacos, prejudica a formação de preços e compromete a isonomia entre participantes. A IOSCO recomenda que os CASPs que atuam como intermediários devem implementar sistemas, políticas e procedimentos que assegurem execução justa, ordenada e célere das ordens de clientes, com proibição de práticas de front-running. Os fatores de best execution incluem preço, custos explícitos e implícitos, velocidade, probabilidade de execução e liquidação, volume e natureza da ordem. Os CASPs que operam ambientes de negociação devem fornecer transparência pré e pós-negociação equivalente à exigida nos mercados tradicionais, incluindo dados de preços, volumes e horários de operações, acessíveis ao público na maior extensão praticável.

agente responsável pela adequação da operação ao perfil do cliente e pela integridade do processo de formação e execução da ordem.

As registradoras podem encontrar na DLT uma infraestrutura que potencializa suas capacidades de rastreabilidade, marcação de gravames e interoperabilidade. A circulação de recebíveis, a cessão fiduciária e a vinculação a financiamentos podem ser facilitadas por contratos inteligentes que executem automaticamente as condições de cessão e liberação.

Os sistemas de liquidação e as contrapartes centrais enfrentam a questão já analisada na seção 3. A liquidação atômica pode eliminar o risco de principal, mas dispensa a compensação multilateral e, com isso, pode ser inadequada para determinados mercados[86].

As cascatas de salvaguardas das CCPs dependem de julgamento institucional que não se automatiza. A CCP pode continuar existindo em ambiente tokenizado como entidade que mutualiza e administra riscos, mesmo que a liquidação operacional migre para a rede.

O risco de contraparte de resgate, discutido na seção sobre liquidação, exige tratamento institucional específico. Quando o token representa um valor mobiliário cuja existência depende de emissor ou de ativo externo à rede, alguém precisa assegurar que o resgate do token resulte efetivamente na entrega do ativo ou no pagamento correspondente.

Essa função pode ser atribuída ao próprio emissor, ao escriturador na qualidade de oráculo, a um custodiante qualificado que detenha o ativo de referência, ou a uma nova categoria de participante que funcione como garantidor do lastro.

[86] Para contratos de derivativos, que possuem vencimento futuro, o risco de contraparte permanece ao longo da vida do contrato, fazendo com que a compensação no modelo atual continue sendo necessária para mitigar riscos. Cf. PRIEM, Randy. Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. *Financial Innovation*, v. 6, n. 1, 2020. Disponível em: https://doi.org/10.1186/s40854-019-0169-6.

A criação de uma infraestrutura específica para essa finalidade é uma hipótese discutida em algumas jurisdições, mas a alternativa mais compatível com o modelo regulatório brasileiro parece ser a atribuição dessa responsabilidade a infraestruturas já existentes, com extensão de seus deveres e requisitos para cobrir o risco de contraparte de resgate.

Ator	Modelo tradicional	Ambiente tokenizado
Custodiante	Guarda de posições em conta	Guarda de chaves criptográficas
Escriturador	Registros originários de titularidade	Função de oráculo da rede
Depositário central	Controle centralizado da titularidade fiduciária	Operador ou co-governante da rede
Administradora de mercado	Negociação e autorregulação	Autorregulação depende de rede permissionada
Corretora e distribuidora	Intermediação e melhor execução	Intermediação simplificada; deveres mantidos
Registradora	Registro de gravames e recebíveis	Rastreabilidade e automação por contratos
CCP e sistema de liquidação	Compensação multilateral e salvaguardas	Liquidação atômica; mutualização permanece

Figura 2 – Reposicionamento dos atores em ambiente tokenizado

Elaboração própria.

8.2.Depositário digital: uma nova figura?

Merece destaque uma proposta para solucionar o problema de garantir que o token corresponda efetivamente ao ativo do mundo real e mitigar os

riscos na liquidação, formulada por Antonio Berwanger[87]. A solução proposta por Berwanger é a criação de uma nova categoria regulatória denominada *depositário digital*.

A proposta rejeita a adoção de sistemas puramente descentralizados para o mercado de capitais e confia a infraestrutura a uma entidade centralizada, autorizada e supervisionada pelo Estado, que será responsável por gerir uma rede de blockchain privada e permissionada.

Para assegurar o lastro e a validade do valor mobiliário representado pelo token, o autor estrutura a solução centrada na função de *gatekeeper* exercida por entidades reguladas.

A depender da origem do ativo, a solução de Berwanger distribui essa responsabilidade em dois segmentos.

Para valores mobiliários existentes fora da rede (ativos escriturais), a solução envolve a manutenção do escriturador tradicional, que continua responsável por controlar o estoque total emitido pela companhia. Quando uma parcela dessas ações é enviada ao mercado, o depositário digital recepciona os ativos e cria os tokens correspondentes na blockchain. Para garantir que o token reflita exatamente o ativo externo (atuando na prática como a ponte com a realidade *off-chain*), Berwanger propõe que o escriturador atue como um nó (node) da rede permissionada gerida pelo depositário digital. Isso permite que o escriturador faça a conciliação em tempo real e valide as operações, assegurando a correspondência fiel do token.

Para valores mobiliários criados diretamente na rede (nato-digitais), como o ativo não possui um registro escritural prévio no mundo exterior, o próprio depositário digital assume integralmente os deveres de diligência

[87] BERWANGER, Antonio Carlos. *Tokenização de valores mobiliários: a digitalização em redes de blockchain como alternativa à emissão e à cadeia de pós-negociação tradicional em mercados organizados de valores mobiliários*. 2025. Dissertação (Mestrado em Direito da Regulação) – Fundação Getulio Vargas, Escola de Direito do Rio de Janeiro, Rio de Janeiro, 2025.

(*gatekeeper*), responsabilizando-se por verificar a regularidade da emissão e a efetiva validade jurídica e material do ativo tokenizado.

Para além da verificação da existência do ativo, a solução exige um arcabouço de controle rigoroso para garantir que o resgate e a liquidação (DvP) ocorram sem falhas. Isso é obtido por meio de dois pilares adotados pelo depositário digital.

Primeiramente, a titularidade fiduciária. O depositário digital detém a propriedade fiduciária dos ativos, o que garante controle absoluto sobre eles e blinda o patrimônio dos investidores contra eventuais reivindicações de credores caso a instituição sofra insolvência.

Em segundo lugar, o controle das chaves privadas. A entidade operadora da rede detém e gerencia as chaves privadas das carteiras (*wallets*) dos investidores.

Ao centralizar esse controle, o depositário digital impede que o investidor aliene o token fora do ambiente de mercado (prevenindo o gasto duplo) e garante que ele seja o único capaz de executar a transferência do token de forma vinculada e simultânea ao pagamento.

Portanto, Berwanger não delega a garantia do ativo a oráculos descentralizados, mas sim confia a ancoragem da realidade *off-chain* ao escriturador (operando como um nó validador) e atribui a responsabilidade estrutural de segurança, custódia e diligência ao depositário digital.

8.3.Arquiteturas unificadoras

O Unified Ledger proposto pelo BIS [88] parte da premissa de que a fragmentação entre redes distintas é o principal obstáculo à adoção institucional de DLT em mercados financeiros.

[88] BANK FOR INTERNATIONAL SETTLEMENTS (BIS). *BIS Annual Economic Report 2023*: III. Blueprint for the future monetary system: improving the old, enabling the new. Basel, 2023. Disponível em https://www.bis.org/publ/arpdf/ar2023e3.pdf. A formulação original do BIS

A proposta consiste em uma plataforma única, operada ou supervisionada por autoridades, na qual coexistam representações tokenizadas de moeda de banco central, depósitos bancários tokenizados e ativos financeiros tokenizados. A liquidação atômica entre esses componentes é viabilizada pela presença de todos na mesma plataforma, eliminando a necessidade de pontes, oráculos ou reconciliação entre redes.

O modelo tem atratividade conceitual. Ao reunir ativos e moeda em um único ambiente, resolve simultaneamente o problema do ativo de liquidação, da interoperabilidade e da fragmentação. A programabilidade, combinada com moeda de banco central tokenizada, permite automação completa de ciclos de emissão, negociação, liquidação e eventos corporativos.

A proposta do BIS não se resume à liquidação de ativos tokenizados, mas pressupõe desenho jurídico-regulatório, modularidade, verificabilidade, privacidade, escalabilidade e governança evolutiva, de modo que o *ledger* unificado é tratado como bloco construtivo de uma reorganização mais ampla da infraestrutura financeira digital[89].

As limitações são igualmente relevantes. A concentração de todos os ativos e moedas em uma única plataforma cria um ponto de falha sistêmico de proporções inéditas.

Unified Ledger aparece aqui como proposta de uma nova infraestrutura de mercado financeiro em que moeda do banco central, moedas privadas tokenizadas e outros ativos tokenizados coexistem na mesma plataforma programável, permitindo composabilidade (*composability*), programabilidade e liquidação atômica multiativos; o argumento central é que o ganho econômico não decorre apenas da digitalização de ativos, mas da reunião, no mesmo ambiente ("*venue*"), dos objetos transacionados, das regras de execução e da camada informacional necessária para autenticação, condicionalidade e liquidação final, preservando ainda a estrutura monetária em dois níveis e admitindo, contra uma leitura maximalista, a coexistência de múltiplos *ledgers* conectados por APIs.

[89] CARSTENS, Agustín; NILEKANI, Nandan. *Finternet*: the financial system for the future. BIS Working Papers, Basel, n. 1178, 2024. Disponível em https://www.bis.org/publ/work1178.htm. O texto amplia o horizonte do Unified Ledger ao inseri-lo na arquitetura mais ampla do Finternet, isto é, um ecossistema financeiro interoperável e orientado ao usuário, no qual *ledgers* unificados funcionam como veículos institucionais para conectar serviços, ativos e intermediários antes segregados.

A governança dessa plataforma é complexa, porque envolve múltiplas autoridades, jurisdições e categorias de participantes com interesses potencialmente conflitantes[90]. A exigência de que todos os participantes migrem para um único ambiente pode gerar custos de transição elevados e resistência de incumbentes. E a compatibilidade com o princípio de que diferentes jurisdições mantêm soberania sobre suas infraestruturas financeiras não é trivial.

Por seu turno, as Redes de Responsabilidade Regulada (*Regulated Liability Networks*, RLN) adotam premissa diferente[91]. Em vez de uma plataforma única, propõem uma rede de redes na qual cada participante opera seu próprio nó ou rede, sujeito à regulação de sua jurisdição, mas interconectado com os demais por protocolos padronizados e regras comuns de interoperabilidade.

Cada ativo tokenizado carrega consigo a identificação do regime regulatório a que está sujeito e da entidade responsável pelo seu lastro. A liquidação entre redes distintas é viabilizada por mecanismos de coordenação que preservam a finalidade (*settlement finality*), sem exigir que todos os ativos residam na mesma plataforma.

---

[90] BALLASCHK, David et al. Think globally, settle locally? Multilateral platforms for cross-border payments based on DLT. *Journal of Payments Strategy & Systems*, v. 18, n. 2, p. 127-138, 2024. Disponível em: https://ideas.repec.org/a/aza/jpss00/y2024v18i2p127-138.html. Para os autores, os maiores obstáculos para a sua implementação não são tecnológicos, mas sim políticos e de governança. A criação de uma única plataforma multilateral global é irrealista e que o mercado deve focar no desenvolvimento de soluções regionais interligadas.

[91] CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE (CCAF). *Tokenised Money*: Use Cases, Interoperability and Regulation. Cambridge: University of Cambridge Judge Business School, 2026. Disponível em https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/tokenised-money-use-cases-interoperability-and-regulation/. O relatório mostra a evolução do conceito de RLN para iniciativas posteriores de interoperabilidade e liquidação, observando que a Regulated Settlement Network se constrói sobre experiências anteriores de RLN e busca permitir liquidação em tempo real de passivos regulados e ativos tokenizados em ambiente compartilhado; ao mesmo tempo, a fonte evidencia que os ganhos demonstrados em provas de conceito ainda convivem com questões abertas de integração, escalabilidade transfronteiriça e governança, o que reforça a leitura de RLN como arquitetura em transição entre desenho conceitual, experimentação de mercado e possível institucionalização regulatória.

Esse modelo é mais compatível com a estrutura atual do sistema financeiro, em que diferentes infraestruturas operam sob supervisão de diferentes autoridades e em diferentes jurisdições. Sua limitação é que a interoperabilidade efetiva depende de padronização, que por sua vez depende de coordenação internacional.

Em setembro de 2024, a UK Finance publicou três relatórios finais detalhando os resultados da Fase de Experimentação da Regulated Liability Network (RLN) no Reino Unido . O projeto colaborativo envolveu 11 instituições financeiras (incluindo Barclays, Citi, HSBC e Lloyds Banking Group) e empresas de tecnologia, com o objetivo de testar e validar o conceito de uma nova Infraestrutura de Mercado Financeiro (FMI) focada em dinheiro digital regulamentado[92].

A fase de experimentação demonstrou a viabilidade técnica da plataforma por meio da implementação de 14 capacidades fundamentais, incluindo pagamentos programáveis, bloqueio e desbloqueio de fundos e orquestração de sequências de pagamento, as quais foram validadas em cinco casos de uso principais.

No *marketplace* P2P, evidenciou-se a mitigação de riscos com retenção de recursos até a confirmação da entrega, Na compra de imóveis, foi possível sincronizar pagamentos múltiplos com a transferência de titularidade, reduzindo tempo e complexidade, No *gateway* de e-commerce, comprovou-se a viabilidade de pagamentos *pull* em diferentes maneiras. Na integração com cartões e PoS, verificou-se compatibilidade com infraestruturas existentes, permitindo o uso de depósitos tokenizados em pontos de venda tradicionais.

[92] Os relatórios Summary Report, Technical Report e Business Report podem ser obtidos em https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/rln-reports-2024. Um princípio basilar que permeia todos os relatórios é a manutenção da Unicidade do Dinheiro (*Singleness of Money*). A plataforma garante que os depósitos tokenizados continuem sendo uma evolução do dinheiro de banco comercial, mantendo a paridade de valor com as moedas emitidas pelo banco central, evitando a fragmentação do sistema monetário.

Por fim, na liquidação de títulos tokenizados, alcançou-se DvP atômico e sincronizado entre ativos tokenizados, depósitos tokenizados e moeda de banco central no atacado.

Apesar dos resultados satisfatórios, foram identificadas algumas preocupações: (i) barreiras regulatórias a serem superadas; (ii) necessidade de potencializar o necessário efeito de rede para adesão dos participantes ao arranjo; (iii) complexidade da integração com os sistemas legados das instituições financeiras; (iv) ampliação de testes de requisitos não funcionais para pagamentos com cartões (especialmente no tocante à latência); e (v) mitigação do risco de fragmentação de liquidez.

A experiência histórica com padronização de infraestruturas financeiras, como a adoção de padrões ISO 20022 para mensageria, sugere que esse processo é lento, incremental e sujeito a resistências[93].

Para a regulação brasileira, tanto o Unified Ledger quanto as RLN funcionam como referências conceituais, não como modelos prontos para adoção.

A articulação com o projeto Drex, que opera como plataforma de liquidação em moeda digital de banco central em rede permissionada,

[93] BURGER, Christian; HOLLANDERS, Auke; KOKKOLA, Tom. *The future of retail payments*: opportunities and challenges. Frankfurt am Main: European Central Bank, 2011. Disponível em https://www.ecb.europa.eu/press/conferences/html/ecb_oenb.en.html. Os autores sustentam a ideia de que a padronização em infraestrutura financeira não ocorre por salto, mas por acumulação lenta de harmonizações parciais em instrumentos, regras, padrões e sistemas. Cf. também RADANOVIC, Ivan. *Payment systems migration to the ISO 20022 electronic messaging standard*. Belgrade: National Bank of Serbia, 2024. Disponível em https://ideas.repec.org/p/nsb/bilten/20.html. Esse estudo examina a migração como processo operacional concreto e não como ideal abstrato de interoperabilidade. Ao descrever experiências internacionais, a transição via rede SWIFT e o caso sérvio, o autor mostra que a mudança do ISO 15022 para o ISO 20022 exige períodos de coexistência, serviços de tradução, adaptação de plataformas e planejamento voltado à continuidade operacional. A ênfase em mensagens maiores, requisitos ampliados de AML/CFT, KYC e prevenção à fraude, bem como na necessidade de compatibilização com outras infraestruturas e escopos regionais, evidencia que a padronização amplia capacidades, mas também eleva custos de migração e coordenação; por isso, a experiência histórica apontada pela literatura é a de um processo lento, incremental e sujeito a fricções técnicas e organizacionais.

posiciona o Brasil em um caminho que combina elementos de ambos os modelos, com CBDC de atacado em rede controlada pelo Banco Central e possibilidade de integração com redes de ativos tokenizados operadas por participantes regulados.

8.4.Arquiteturas híbridas

A alternativa mais provável no curto e médio prazo não é a migração integral para redes distribuídas, mas a adoção de arquiteturas híbridas em que a DLT opera em camadas e funções específicas, convivendo com sistemas legados.

Nesse modelo, a emissão e o registro de titularidade de determinados ativos podem ocorrer em rede distribuída, enquanto a liquidação financeira segue utilizando o SPB. A custódia pode ser exercida por entidades autorizadas que operem tanto em ambiente tradicional quanto em ambiente tokenizado. A negociação pode ocorrer em mercados organizados que utilizem DLT como camada de registro, mas preservem suas regras de acesso, formação de preços e autorregulação.

Essa abordagem tem a vantagem de permitir experimentação incremental, sem exigir ruptura com a infraestrutura existente. Os participantes podem testar a tecnologia em segmentos específicos, como títulos de renda fixa de menor complexidade ou cotas de fundos fechados, antes de estendê-la a mercados de maior volume e liquidez.

Substituir os sistemas legados de uma só vez exigiria investimentos maciços e traria riscos operacionais severos, além de instabilidade potencial para as redes durante a migração. Uma arquitetura híbrida permite uma transição modular, aliviando o fardo de modernizar instituições que operam com sistemas de décadas de idade[94].

[94] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *Tokenisation of assets and distributed ledger technologies in financial markets*: potential impediments

Os custos de transição são menores, porque a infraestrutura existente continua operando em paralelo. E a regulação pode ser adaptada de forma gradual, com dispensas ou regimes experimentais para os segmentos tokenizados, sem necessidade de reformulação integral do arcabouço normativo.

Os riscos da abordagem híbrida são de outra natureza. A convivência de dois ambientes operacionais gera necessidade de reconciliação entre eles, o que pode anular parte dos ganhos de eficiência que a DLT prometia.

A complexidade regulatória aumenta, porque é preciso definir qual regime se aplica a cada camada e como se tratam as interfaces. E a fragmentação de liquidez pode se agravar se ativos semelhantes forem negociados simultaneamente em ambiente tokenizado e em ambiente tradicional, sem mecanismos de arbitragem eficientes entre os dois.

A avaliação crítica da pertinência da DLT, nesse cenário, passa por uma pergunta pragmática. Para cada função e para cada classe de ativo, a introdução de DLT *gera ganhos líquidos* em relação ao arranjo existente, considerados os *custos de transição, os riscos adicionais e a complexidade regulatória*?

A resposta não é uniforme. Para ativos nativamente digitais, emitidos e negociados inteiramente em rede, os ganhos tendem a ser claros. Para ativos já operados em infraestruturas maduras, com alta liquidez e processos consolidados, os ganhos marginais podem não justificar os custos de migração.

Para ativos de menor porte, com baixa liquidez e emissores que enfrentam custos elevados de acesso à infraestrutura tradicional, a DLT pode oferecer caminho de acesso ao mercado de capitais que o modelo atual não viabiliza a custos razoáveis.

---

to market development and policy implications. Business and Finance Policy Paper, n. 75. Paris, 2025. Disponível em: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/01/tokenisation-of-assets-and-distributed-ledger-technologies-in-financial-markets_be149012/40e7f217-en.pdf.

As implicações para a governança e a autorregulação das entidades administradoras de mercados organizados são transversais a todos esses modelos. Se a negociação migrar, ainda que parcialmente, para ambientes distribuídos, a capacidade de monitoramento, supervisão e sanção precisa acompanhar essa migração.

O mecanismo de ressarcimento de prejuízos, por sua vez, foi concebido para intermediação em mercados organizados tradicionais. Sua extensão a ambientes tokenizados depende de definir quem é o participante responsável pela ação ou omissão que gera o dano, o que é menos evidente quando a intermediação é parcialmente substituída por interação direta com contratos inteligentes.

9. PFMI e infraestruturas baseadas em DLT

Os Princípios para Infraestruturas do Mercado Financeiro (PFMI), formulados pelo CPMI e pela IOSCO, organizam a supervisão, a autorização e a avaliação de IMFs. Embora não tenham força normativa direta, foram incorporados às regulações nacionais e operam como referência analítica para qualquer infraestrutura.

Nesta seção, exploramos em que medida infraestruturas baseadas em DLT atendem a esses princípios e em que pontos a tecnologia exige ajustes de interpretação. O debate ganhou densidade com as orientações do CPMI e da IOSCO sobre arranjos de stablecoins[95]. Embora voltadas a sistemas com função de pagamento, essas orientações tratam de governança, gestão de riscos e liquidação com efeitos que se estendem a outras infraestruturas em DLT.

[95] BANK FOR INTERNATIONAL SETTLEMENTS (BIS); INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS (IOSCO). *Application of the Principles for Financial Market Infrastructures to stablecoin arrangements*. Basileia: BIS/IOSCO, 2022. Disponível em https://www.bis.org/cpmi/publ/d206.htm.

A análise a seguir organiza os 24 princípios em blocos temáticos e os confronta com as seções anteriores. O foco não é reproduzir os princípios, mas examinar como as propriedades da DLT interagem com suas exigências.

9.1.Base jurídica e governança

Os Princípios 1 e 2 exigem base jurídica clara e governança orientada à estabilidade. Em redes DLT, a definição de regras, mudanças de protocolo e admissão de participantes não pode depender apenas de código. Esses elementos precisam estar formalizados em instrumentos com validade jurídica.

Modelos baseados em consenso de validadores ou votação de detentores de tokens não atendem, por si, ao padrão exigido. É necessário identificar responsáveis, prever prestação de contas e estabelecer mecanismos de revisão. As orientações sobre stablecoins reforçam a necessidade de uma entidade juridicamente identificável, sujeita a controle e capaz de intervenção humana em situações críticas.

Assim, o uso de DLT não dispensa uma entidade responsável perante o regulador. Redes permissionadas podem atender a essa exigência, desde que a governança seja formalizada com rigor equivalente ao das infraestruturas tradicionais.

9.2.Gestão integrada de riscos

O Princípio 3 exige um arcabouço integrado de gestão de riscos. Em DLT, o perfil de risco se transforma, mas não se reduz. Riscos operacionais e de liquidez persistem e a eles se somam riscos específicos, como perda de chaves e vulnerabilidades em contratos inteligentes.

Arranjos que combinam múltiplas funções introduzem riscos interdependentes. O relatório do CPMI e da IOSCO sobre aplicação dos PFMI às stablecoins exige avaliação contínua dessas interações e instrumentos de

mitigação coordenados, sobretudo quando funções são distribuídas entre entidades distintas.

Em teoria, a DLT permite monitoramento de transações e saldos em tempo real, o que melhora a visibilidade das exposições. Esse ganho não substitui modelos de risco, cenários de estresse e processos decisórios. A interpretação e a resposta permanecem institucionais à luz dos PFMI.

9.3.Riscos de crédito, colateral e liquidez

Os Princípios 4 a 7 tratam da gestão de exposições de crédito, da qualidade do colateral, dos sistemas de margens e do risco de liquidez. A seção 2.3 analisou os ganhos potenciais da DLT na gestão de garantias, especialmente pela eliminação de reconciliações redundantes e pela automação de chamadas de margem e substituição de colateral por meio de contratos inteligentes.

Esses ganhos são compatíveis com os Princípios 4 a 7, mas não os satisfazem automaticamente. O Princípio 4 exige que a infraestrutura mantenha recursos suficientes para cobrir exposições em cenários plausíveis de estresse. A automação da gestão de colateral pode tornar essa cobertura mais eficiente, mas o dimensionamento dos recursos continua dependendo de modelos de risco calibrados e revisados periodicamente, conforme exige o Princípio 6 para sistemas de margens de CCPs.

O Princípio 5 exige que os ativos aceitos como garantia apresentem baixo risco de crédito, liquidez e mercado. Em ambiente tokenizado, a aceitação de tokens como colateral levanta a questão de saber se o ativo digital atende a esses requisitos. Tokens representativos de valores mobiliários de alta liquidez e baixo risco podem satisfazer o princípio; tokens com liquidez restrita, volatilidade elevada ou risco de contraparte de resgate dificilmente o farão. Os deságios devem refletir não apenas o risco de mercado do ativo subjacente, mas também os riscos específicos do ambiente tokenizado, como a possibilidade de descolamento entre o preço do token e o valor do ativo de referência.

O Princípio 7, relativo ao risco de liquidez, ganha relevância adicional em cenários de liquidação atômica em base bruta, conforme analisado na seção 2.2. A liquidação operação a operação, sem compensação multilateral, aumenta a demanda por liquidez intradiária. A infraestrutura precisa demonstrar que dispõe de recursos líquidos suficientes para cumprir obrigações mesmo quando o volume de operações e a ausência de compensação pressionam as necessidades de caixa.

9.4.Finalidade e segurança da liquidação

Os Princípios 8, 9, 11 e 12 tratam da liquidação. Em DLT, a escolha do mecanismo de consenso é determinante. Mecanismos probabilísticos não atendem à exigência de finalidade. Redes permissionadas podem atender, desde que a finalização seja reconhecida juridicamente.

As orientações sobre stablecoins destacam o risco de desalinhamento entre o estado do registro e a posição jurídica. *Forks* podem comprometer transações validadas. A infraestrutura deve definir o ponto de irrevogabilidade e garantir base jurídica consistente.

A liquidação monetária em moeda de banco central permanece a referência. Stablecoins introduzem risco de crédito e liquidez do emissor e de suas reservas. Por sua vez, CBDCs de atacado oferecem maior aderência ao princípio. No contexto brasileiro, a articulação com o Drex é promissora.

A integridade das emissões exige controle sobre a criação de tokens e governança sobre alterações. A liquidação atômica elimina o risco de principal ao condicionar entrega e pagamento simultâneos.

9.5.Inadimplemento e proteção de clientes

Os Princípios 13 e 14 exigem regras claras para lidar com inadimplência de participantes e mecanismos de segregação e portabilidade de posições de clientes. A seção 2.3 analisou a segregação patrimonial em ambiente

tokenizado, contrastando segregação individual por endereço e segregação *omnibus*. A seção 4 discutiu as cascatas de salvaguardas das CCPs e a dificuldade de automatizar a lógica de mutualização de perdas.

O Princípio 13 exige que a infraestrutura possua procedimentos que permitam ações rápidas para conter perdas e pressões de liquidez em caso de inadimplência. Em ambiente tokenizado, contratos inteligentes podem automatizar parte desses procedimentos, como a liquidação forçada de posições garantidas ou o acionamento de fundos de proteção. A etapa de julgamento institucional, que envolve avaliação da gravidade do inadimplemento, comunicação a autoridades, eventual suspensão de participantes e decisão sobre uso de recursos mutualizados, permanece necessariamente humana e deliberativa.

O Princípio 14 é diretamente favorecido pela segregação individual em rede. Quando os ativos de cada cliente estão registrados em endereços próprios, a portabilidade para outro custodiante pode ser executada de forma mais rápida e transparente do que no modelo atual, em que a transferência depende de múltiplas comunicações entre prestadores. A condição é que o novo custodiante esteja integrado à rede e que os mecanismos de identificação e compliance sejam preservados.

9.6.Riscos empresariais, custódia e risco operacional

Os Princípios 15, 16 e 17 tratam da resiliência institucional da infraestrutura. O Princípio 15 exige identificação de riscos empresariais e manutenção de ativos líquidos para recuperação ou encerramento ordenado. O Princípio 16 exige proteção dos ativos da infraestrutura e de seus participantes. O Princípio 17 exige sistemas tecnológicos seguros, mecanismos de redundância e planos de continuidade.

A seção 3 analisou esses riscos em detalhe. A DLT altera o perfil do risco operacional, introduzindo categorias como perda de chaves, exploração de

contratos inteligentes e bifurcações de rede. A resiliência inerente à distribuição de nós atenua o risco de ponto único de falha, mas a dependência de quórum mínimo de validadores para consenso cria nova modalidade de indisponibilidade sistêmica. Os planos de continuidade precisam contemplar cenários específicos do ambiente distribuído, sem dispensar as exigências que a regulação já impõe para infraestruturas tradicionais.

O Princípio 16, relativo à proteção de ativos, conecta-se diretamente à discussão sobre custódia da seção 2.1. A guarda de chaves criptográficas é o equivalente funcional da guarda de ativos no ambiente tokenizado. Os requisitos de segurança, segregação e backup aplicáveis à custódia tradicional precisam ser reinterpretados para esse novo objeto, com atenção ao fato de que a perda de chave não é corrigível pela conciliação com outras bases.

9.7.Acesso, participação e interconexões

Os Princípios 18 a 20 tratam de acesso e vínculos entre infraestruturas. Redes permissionadas permitem definir critérios objetivos de participação. O desafio surge quando se busca ampliar o acesso além do padrão prudencial tradicional.

A participação indireta, por meio de custodiantes, exige monitoramento de riscos e de concentração. A interoperabilidade entre redes depende de pontes ou padrões comuns. Esses mecanismos precisam atender a requisitos elevados de segurança.

9.8.Eficiência, padronização e transparência

Os Princípios 21 a 24 tratam de eficiência e transparência. A DLT pode reduzir reconciliações, automatizar processos e encurtar ciclos de liquidação. Esses ganhos dependem de escala e não podem ser anulados por fragmentação ou custos de transição.

A padronização é condição para integração. A ausência de padrões de dados e mensageria limita o potencial da tecnologia. A rastreabilidade pode ampliar a transparência, mas exige equilíbrio com proteção de dados e sigilo.

10. Síntese do capítulo

A análise conduzida ao longo deste capítulo permite algumas conclusões.

A primeira é que a DLT não é incompatível com os PFMI, mas tampouco os satisfaz por construção (*by design*). Cada princípio exige avaliação específica da configuração concreta da infraestrutura. Redes permissionadas com finalidade determinística, governança formalizada e integração com moeda de banco central estão mais próximas do atendimento aos princípios. Redes públicas com governança difusa, finalidade probabilística e liquidação em ativos privados estão mais distantes.

A segunda é que a DLT oferece ganhos reais em domínios específicos. A liquidação atômica elimina o risco de principal de forma estrutural. A gestão de colateral em livro-razão compartilhado reduz reconciliações e pode permitir operação com níveis de garantia mais próximos do risco efetivo. A segregação individual por endereço reforça a proteção patrimonial e a portabilidade. A rastreabilidade nativa amplia a capacidade de supervisão e auditoria.

A terceira é que esses ganhos convivem com riscos e limitações igualmente reais. A perda de chaves é irreversível. Contratos inteligentes são difíceis de corrigir após implantação. A fragmentação entre redes pode anular os benefícios de interoperabilidade. A governança de redes distribuídas exige formalização institucional que a tecnologia, por si, não fornece. E as funções de julgamento, deliberação e coordenação em cenários de crise permanecem humanas e institucionais.

A quarta conclusão é que o trilema da DLT conduz, na prática, a infraestruturas que preservam ganhos de automação, rastreabilidade e

compartilhamento de dados, mas operam com grau limitado de descentralização. Essa configuração é menos revolucionária do que o discurso original da DLT sugere, mas é a que se mostra viável para ambientes regulados.

A quinta é que a arquitetura mais provável no curto prazo é híbrida, com DLT operando em camadas e funções específicas, convivendo com sistemas legados. A migração integral para redes distribuídas depende de condições que ainda não se verificam plenamente, como padronização internacional, disponibilidade de CBDC de atacado para liquidação e maturação da governança de redes.

A pergunta que resta é como a regulação brasileira pode criar espaço para essa experimentação sem comprometer as funções institucionais que as IMFs exercem e sem antecipar escolhas tecnológicas que o mercado ainda não consolidou.

11. Resumo

O caderno investiga se, e em que condições, o uso de *Distributed Ledger Technology* (DLT) pode reorganizar funções das infraestruturas do mercado financeiro (IMFs) sem comprometer as funções institucionais que as justificam. Ineficiências como o ciclo T+2, a reconciliação de bases fragmentadas e a sobreposição funcional entre prestadores são custos reais de coordenação. As infraestruturas centrais, porém, institucionalizam confiança, internalizam riscos sistêmicos e coordenam respostas a inadimplementos, funções que um protocolo não substitui.

As decisões de arquitetura condicionam essa avaliação. A camada e o tipo de rede, o mecanismo de consenso, o ativo de liquidação, a interoperabilidade e os contratos inteligentes determinam se a infraestrutura pode ser ambiente de liquidação definitiva. Redes permissionadas com consenso de tolerância bizantina a falhas oferecem finalidade determinística, compatível com o Princípio 8 dos PFMI, ao contrário das redes públicas de consenso probabilístico.

Na custódia e no depósito centralizado, ambas as atividades passam a operar sobre a chave criptográfica que movimenta o token, aproximando-se operacionalmente sem eliminar a distinção regulatória. Os modelos vão da custódia plena à autocustódia, com armazenamento em carteiras frias, quentes e mornas. A guarda e a gestão de chaves tornam-se a função nuclear, pois a perda da chave implica perda irreversível do ativo. A emissão e a queima de tokens equivalem à constituição e à extinção do depósito, e as provas de reservas, ativos, passivos e solvência permitem verificação contínua. A combinação com *staking* e empréstimo de ativos (*lending*) adiciona riscos que exigem segregação e informação ao cliente.

A liquidação é o ponto de maior tensão. O ativo de liquidação pode ser moeda fiduciária no Sistema de Pagamentos Brasileiro ou representações

tokenizadas de moeda, como *stablecoins*, depósitos tokenizados ou moedas digitais de banco central, cuja escolha depende da evolução do projeto Drex. A finalidade exigida é determinística, e o risco de contraparte de resgate persiste quando o token depende de instituição externa. A liquidação atômica elimina o risco de principal, mas dispensa a compensação multilateral e eleva a demanda por liquidez intradiária, exigindo soluções intermediárias.

A gestão de garantias e a proteção patrimonial reconfiguram-se sem dispensar a arquitetura regulatória. O livro-razão compartilhado elimina reconciliações redundantes, ainda que nem toda reconciliação seja dispensável. A segregação individual por endereço reforça a proteção contra insolvência frente à segregação omnibus, e os seguros funcionam como mecanismo complementar. Formadores de mercado automatizados e exchanges descentralizadas oferecem provisão alternativa de liquidez, com riscos como a perda impermanente e a ausência de intermediário regulado.

Em dados e interoperabilidade, o livro-razão comum converte a reconciliação periódica em verificação contínua, mas o risco de fragmentação exige pontes ou padrões comuns. A rastreabilidade nativa colide com obrigações de sigilo, e o modelo on-chain e off-chain, apoiado em oráculos, delimita o que reside na rede. Credenciais verificáveis podem viabilizar a portabilidade de KYC sem reduzir o rigor das obrigações de identificação.

O trilema da DLT indica que a descentralização tende a ser o vértice sacrificado em ambientes regulados, e os impedimentos ao desenvolvimento de mercado sistematizados pela OCDE mostram que a maioria dos limites não é estritamente regulatória. Entre as arquiteturas possíveis, o caderno examina o reposicionamento dos atores, a proposta de depositário digital, os modelos unificadores como o *Unified Ledger* e as Redes de Responsabilidade Regulada, e as arquiteturas híbridas, tidas como as mais prováveis no curto prazo. A DLT não é incompatível com os PFMI, mas tampouco os satisfaz por construção, e as

funções de deliberação e coordenação em cenários de crise permanecem humanas e institucionais.