RISCOS NA ADOÇÃO DE MOEDAS DIGITAIS FIDUCIÁRIAS
Integração necessária de novas tecnologias ao sistema de segurança jurídica nacional.*

RESUMO

Este artigo analisa os principais riscos associados à implementação de Moedas Digitais de Banco Central (CBDCs - *Central Bank Digital Currency*, no inglês), com ênfase no projeto Drex brasileiro. A pesquisa evidencia a necessidade de preservação e integração do sistema constitucional de registros públicos brasileiro com as novas tecnologias blockchain, em vez de sua substituição. São analisados riscos jurídicos, operacionais, tecnológicos e geopolíticos, com destaque para as ameaças emergentes da computação quântica. Conclui-se que um modelo híbrido de implementação, com a manutenção do sistema de registros públicos com base constitucional, a ele incorporando tecnologias blockchain como camada complementar, representa a alternativa mais segura para a modernização do sistema financeiro brasileiro, em padrões de segurança jurídica, segurança nacional e inclusão de todos os estratos sociais.

Palavras-chave: Moedas Digitais de Banco Central. Drex. Registros Públicos. Blockchain. Segurança jurídica. Segurança nacional. Privacidade. Computação Quântica.

1 INTRODUÇÃO

A crescente digitalização do sistema financeiro global tem impulsionado diversos bancos centrais a desenvolver suas próprias moedas digitais. No Brasil, o desenvolvimento do Real Digital (Drex) representa um passo significativo na modernização do sistema financeiro nacional, mas também suscita questões fundamentais sobre sua implementação, segurança e impactos.

Este artigo busca analisar criticamente os riscos associados à implementação do Drex, especialmente no que tange à proposta de substituição do sistema de registros públicos existente por registros em blockchain geridos por empresas privadas. A análise parte da premissa constitucional de que o sistema brasileiro de registros públicos, previsto no artigo 236 da Constituição Federal, constitui pilar fundamental do sistema de segurança jurídica nacional, e deve ser preservado e integrado às novas tecnologias, nunca descartado.

2 FUNDAMENTAÇÃO TEÓRICA E EXPERIÊNCIAS INTERNACIONAIS

2.1 Conceituação e Modelos de CBDCs

As Moedas Digitais de Banco Central representam a forma digital da moeda fiduciária nacional, emitida e garantida pela autoridade monetária. Diferentemente das criptomoedas privadas, as CBDCs são instrumentos oficiais que mantêm as características fundamentais do dinheiro tradicional: meio de troca, unidade de conta e reserva de valor (BANK FOR INTERNATIONAL SETTLEMENTS, 2023).

Os modelos de implementação variam significativamente entre países, podendo ser classificados em:

a) **Modelos de varejo (retail)**: direcionados ao público geral;
b) **Modelos de atacado (wholesale)**: limitados a instituições financeiras;
c) **Modelos híbridos**: combinando características dos dois anteriores.

Cada modelo implica diferentes desafios técnicos, jurídicos e operacionais, exigindo análise contextualizada para cada sistema financeiro nacional.

2.2 Lições das Implementações Internacionais

A análise das experiências internacionais fornece importantes lições para o desenvolvimento do Drex. Casos como o eNaira nigeriano ilustram os riscos de implementações apressadas:

> O eNaira, lançado em outubro de 2021, enfrentou resistência generalizada da população, problemas técnicos recorrentes e baixíssima taxa de adoção (menos de 0,5% da população), evidenciando os riscos de implementações que não consideram adequadamente o contexto socioeconômico local (AYANDELE, 2023, p. 78).

Por outro lado, experiências como o Sand Dollar das Bahamas e o e-CNY chinês demonstram que abordagens graduais e planejadas tendem a obter melhores resultados:

> O e-CNY chinês, em desenvolvimento desde 2014 e em testes extensivos desde 2020, adotou uma abordagem incremental com testes em múltiplas cidades, integrando-se gradualmente ao ecossistema de pagamentos existente e mantendo compatibilidade com sistemas tradicionais (PEOPLE'S BANK OF CHINA, 2023, p. 45).

3 O SISTEMA BRASILEIRO DE REGISTROS PÚBLICOS E SUA BASE CONSTITUCIONAL

3.1 Fundamentos Constitucionais e Legais do Sistema Registral Brasileiro

O sistema brasileiro de registros públicos encontra seu alicerce no artigo 236 da Constituição Federal, que estabelece:

> Art. 236. Os serviços notariais e de registro são exercidos em caráter privado, por delegação do Poder Público (BRASIL, 1988).

Este dispositivo estabelece um modelo peculiar de prestação de serviço público por delegação, submetido a regime jurídico específico que combina elementos públicos e privados. O sistema

é complementado por um arcabouço legal robusto, que inclui a Lei 8.935/94 (Lei dos Cartórios) e a Lei 6.015/73 (Lei de Registros Públicos).

Um aspecto importantíssimo desse sistema é que as funções registrais são exercidas por agentes delegados pelo estado, independentes, mas cuja atividade é normatizada e fiscalizada pelo Poder Judiciário, aos quais, por isso mesmo, é conferida fé pública, elemento essencial para conferir higidez ao sistema.

Lado outro, além de não atenderem à previsão constitucional para o exercício das atividades notariais e de registro, empresas privadas não gozam de independência, não estão submetidas a normas ou fiscalização pelo Poder Judiciário, e não ostentam fé pública, de modo que em face de eventuais irregularidades que sejam alegadas por usuários, o ônus da prova quanto à regularidade da sua ação caberia a elas, o que inviabilizaria um normal funcionamento do sistema, levando a uma crescente judicialização, emperrando o que deve fluir.

3.2 Características Fundamentais e Garantias do Sistema

O sistema registral brasileiro possui características essenciais que garantem segurança jurídica às relações sociais e econômicas:

a) **Fé pública**: os atos praticados pelos registradores gozam de presunção de veracidade, o que opera a inversão do ônus da prova quanto a alegadas irregularidades, dotando o sistema de importante salvaguarda contra atitudes desarrazoadas de usuários;

b) **Estabilidade jurídica**: a jurisprudência consolidada sobre o sistema registral proporciona previsibilidade;

c) **Responsabilidade pessoal**: os registradores respondem diretamente pelos atos praticados;

d) **Fiscalização judicial**: supervisão direta pelo Poder Judiciário;

e) **Capilaridade territorial**: grande número de ofícios de registros públicos com presença em todos os municípios brasileiros, o que é importantíssimo, tanto segundo o aspecto de dar suporte à população mais carente de acesso a recursos tecnológicos - a maioria da população brasileira -, quanto sob o aspecto tecnológico, porque permite dotar a rede blockchain de grande número de "nós", o que é importantíssimo para a segurança dessa tecnologia;

f) **Qualificação jurídica**: análise técnico-jurídica dos atos e documentos;

g) **Conservação permanente**: guarda perpétua dos documentos e registros.

Como observa Ricardo Dip (2022, p. 67), "o sistema registral brasileiro constitui elemento essencial da segurança jurídica nacional, tendo evoluído continuamente para incorporar inovações tecnológicas sem comprometer sua finalidade pública fundamental".

3.3 Evolução Tecnológica do Sistema Registral

Contrariamente à percepção de um sistema anacrônico, os registros públicos brasileiros têm incorporado continuamente inovações tecnológicas:

a) Implantação do Sistema Eletrônico dos Registros Públicos - SERP, com a generalização dos registros eletrônicos e centralização, em um único portal na WEB, do acesso aos ofícios de registros públicos de todas as especialidades - registro de títulos e documentos e civil de pessoas jurídicas, registro de imóveis e registro civil das pessoas naturais;
b) Implementação dos operadores nacionais de cada especialidade de registro público, integrados ao SERP, o que está permitindo ao sistema grande evolução tecnológica;
c) Adoção de assinaturas digitais e certificação digital.

Estas iniciativas demonstram a capacidade do sistema de evoluir tecnologicamente sem comprometer sua base constitucional e suas garantias fundamentais.

4 ANÁLISE CRÍTICA DA PROPOSTA DE SUBSTITUIÇÃO POR REGISTROS EM BLOCKCHAIN A SEREM REALIZADOS POR EMPRESAS PRIVADAS

4.1 Propostas de Implementação do Drex

O projeto Drex do Banco Central do Brasil propõe a utilização de tecnologia blockchain para diversos fins, incluindo:

a) Emissão da moeda digital;
b) Tokenização de ativos reais e financeiros;
c) Registro e transferência de propriedades;
d) Execução de contratos inteligentes.

Algumas vertentes do projeto sugerem que o registro exclusivamente em blockchain poderia potencialmente substituir o sistema tradicional de registros públicos, argumentando ganhos de eficiência e redução de custos (BANCO CENTRAL DO BRASIL, 2023), como se uma coisa - a adoção das novas tecnologias - fosse impossível sem o descarte da outra, o Sistema Brasileiro de Registros Públicos, o que decididamente não é verdade, muito pelo contrário.

Na realidade, a idéia de que o Sistema Brasileiro de Registros Públicos seria incompatível com a adoção da novas tecnologias digitais - *blockchain*, *smart contracts,* tokenização de ativos - é “vendida" à sociedade brasileira por uma maldisfarçada ação de grupos privados que cobiçam assumir as atividades públicas essenciais realizadas pelos ofícios de registros públicos, alheias ao interesse público, focando apenas na obtenção de grandes lucros, pela concentração da atividade em algumas poucas empresas, ignorando a necessidade de independência, submissão a normas administrativas e de fiscalização do sistema de segurança jurídica nacional, exercida pelo Poder Judiciário, inclusive, a necessidade de suporte em sólido arcabouço jurídico, de base constitucional.

Muito pelo contrário, a utilização da estrutura brasileira de registros públicos, através do SERP - Sistema Eletrônico dos Registros Públicos, dotará o sistema de muito mais segurança tecnológica e jurídica.

Segurança tecnológica, porque proverá uma maior rede distribuída de “nós” para a blockchain do sistema, o que será essencial para lhe reduzir a vulnerabilidade a ataques, bem como porque dotará o sistema de redundância, pela simultânea manutenção dos registro eletrônico atualmente já utilizado pelos Ofícios de registros públicos.

E segurança jurídica porque o sistema brasileiro de registros públicos é submetido a rígidas normas e fiscalização pelo Poder Judiciário, é resiliente e dotado de experimentado sistema de solução de conflitos, correção de erros, etc, essenciais para que o sistema funcione a contento.

Adicione-se a tudo isso o importantíssimo suporte que dará à esmagadora maioria da população brasileira não versada e sem acesso a tecnologias digitais, o que será essencial, não só para que a exclusão digital não se transforme em negativa de direitos constitucionalmente previstos, como, também, para que não incorramos no fracasso ocorrido na Nigéria com a implantação da sua moeda fiduciária digital.

Finalmente, é importante ressaltar que o sistema brasileiro de registros públicos é descentralizado, não concentrando, portanto, decisões e ações, o que não só lhe confere maior segurança, como é importante elemento da cidadania e democracia em nosso país, e emprega muitos milhares de colaboradores, que serão descartados, se tudo passar a ser concentrado em poucas empresas, no âmbito do Sistema Financeiro Nacional, sem submissão a normas administrativas de execução e fiscalização emanadas do Poder Judiciário, guardião da segurança jurídica em nosso país.

A centralização da execução dos serviços de registros em poucas empresas do ecossistema do Sistema Financeiro Nacional, onde pontifica o grande capital privado nacional, afigura-se mesmo uma temeridade, não apenas sob o aspecto da segurança jurídica, já que agentes ligados aos credores não teriam a necessária isenção e independência para tal atividade, como, também, sob o aspecto dos direitos e liberdades, porque permitiria muito fácil violação de privacidade, ações repressoras a cidadãos e/ou empresas, que ficariam reféns do estado e seus gestores da ocasião, restando vulneradas as garantias constitucionais de privacidade, liberdade, direitos e cidadania, e, em última instância, restaria vulnerada a própria democracia.

4.2 Riscos Jurídico-Constitucionais da Substituição

A substituição do sistema registral atual por registros privados em blockchain apresenta riscos jurídicos significativos:

4.2.1 Questionamentos Constitucionais

A delegação constitucional dos serviços registrais não pode ser simplesmente ignorada ou contornada por regulamentação infralegal. Como observa Lamana Paiva (2023, p. 112):

> A substituição do sistema constitucional de registros públicos por mecanismos alternativos sem adequada base constitucional representaria não apenas uma violação direta do artigo 236 da CF, mas uma fragilização do próprio Estado de Direito, ao ignorar os mecanismos formais de alteração constitucional e de leis, porque tudo estaria apenas submetido a normas baixadas pelo Banco Central do Brasil, à margem do Poder Legislativo e, depois, à margem do Poder Judiciário, a quem constitucionalmente cabe normatizar administrativamente e fiscalizar atividades de natureza notarial e registral.

Resumindo, todo o modelo do sistema de segurança jurídica do país, experimentado há séculos, no Brasil e no mundo, seria deixado de lado, para uma aventura irresponsável, que colocaria em risco não apenas o patrimônio das pessoas físicas e jurídicas do país, mas também a própria segurança e a soberania nacional, que poderiam ser solapadas da noite para o dia, em face de algum ataque cibernético. E aqui cabe lembrar que redes blockchain com poucos nós apresentam grande vulnerabilidade, já tendo sido alvo, de muitas violações.

E a verdade é que a substituição do sistema brasileiro de registros públicos por empresas privadas não é necessária para que sejam implementados os registros em blockchain, a tokenização de ativos e a utilização de *smart contracts,* porque todas essas funcionalidades podem ser implantadas com suporte no experimentado sistema de segurança jurídica do país, constitucionalmente previsto no art. 236 da Constituição Federal, para ser operado por agentes independentes do estado e do capital privado, por profissionais do direito dotados de fé pública, atuando sob normas legas impostas pelo Poder Legislativo e rígidas normas administrativas e de fiscalização realizadas pelo Poder Judiciário.

Utiliza-se a necessidade de adoção dessas modernas tecnologias como justificativa para solapar todo o sistema de segurança jurídica do país e entregar a execução de registros públicos e funções tabelioas a grupos privados, representantes do grande capital, que de há muito cobiçam exercer essas atividades, tão somente com o objetivo de obter enormes lucros, em prejuízo do interesse público de toda a sociedade brasileira, gerando o desemprego de milhares de colaboradores nas serventias extrajudiciais e lançando nosso país em uma aventura no desconhecido.

O sistema notarial e de registros públicos brasileiro pode realizar toda essa modernização com muitas vantagens, inclusive com redundância em seus sistemas eletrônicos atualmente utilizados.

4.2.2 Lacunas de Regulamentação

A ausência de um marco legal abrangente para registros em blockchain cria um vácuo normativo preocupante:

a) Indefinição sobre a natureza jurídica dos registros em blockchain;
b) Ausência de regras claras sobre responsabilidade civil;
c) Incertezas quanto a mecanismos de resolução de conflitos;
d) Indefinição sobre custódia e preservação de longo prazo.

Nenhuma dessas incertezas haverá se essas novas tecnologias forem implementadas com suporte no sistema brasileiro de segurança jurídica, composto por notários e registradores, com imensa estrutura já existente, expertise, jurisprudência e capacidade para operar a profilaxia dos problemas acima referidos.

4.2.3 Fragmentação Normativa

A possível coexistência de sistemas paralelos poderia resultar em:

a) Conflitos entre registros tradicionais e registros em blockchain;
b) Insegurança sobre a prevalência em caso de divergências;
c) Dificuldades na aplicação de decisões judiciais;
d) Arbitragem regulatória e *forum shopping* (escolha do órgão julgador mais favorável às teses do autor).

4.3 Riscos Operacionais e Técnicos

4.3.1 Vulnerabilidades da Tecnologia Blockchain

Apesar de suas vantagens, a tecnologia blockchain apresenta vulnerabilidades significativas:

a) **Ataques de 51%**: em blockchains permissionadas com número limitado de validadores, como seria o caso do Drex, o risco de conluio entre validadores é significativo;

Obs: "Ataque de 51%" é a circunstância em que um grupo de validadores, em uma rede blockchain, obtém o controle de mais que 50% da taxa de hash de mineração da rede, o que lhes permite manipular e violar a rede de várias formas, inclusive revertendo transações.

b) **Falhas em contratos inteligentes**: como demonstrado em diversos incidentes em blockchains públicas, porque contratos inteligentes podem conter vulnerabilidades críticas;

c) **Problemas de escalabilidade**: limitações de desempenho em situações de alto volume de transações;

d) **Riscos de chaves privadas**: a perda de chaves privadas pode resultar na impossibilidade permanente de acesso aos ativos.

4.3.2 Desafios de Governança Tecnológica

A implementação de sistemas blockchain para registros públicos enfrenta desafios significativos de governança:

a) Definição sobre autoridade para alterações de protocolo;
b) Mecanismos de atualização e correção de vulnerabilidades;
c) Protocolos de contingência para falhas sistêmicas;
d) Responsabilidade por erros ou violações de segurança.

4.3.3 Problema da Irreversibilidade

Uma característica fundamental dos blockchains é a imutabilidade dos registros, o que pode representar uma desvantagem significativa em contextos que exigem flexibilidade:

a) Dificuldade ou impossibilidade de corrigir erros;
b) Desafios na implementação de decisões judiciais;
c) Complexidade na aplicação de institutos como usucapião, desapropriação ou anulação de negócios jurídicos diversos, incluindo bem móveis ou imóveis.

4.4 Riscos Sociais e de Acesso

4.4.1 Exclusão Digital

A migração para sistemas exclusivamente digitais pode aprofundar desigualdades existentes:

a) Barreiras de acesso para populações sem alfabetização digital;
b) Dificuldades em áreas com infraestrutura tecnológica deficiente;
c) Exclusão de pessoas sem acesso a dispositivos adequados.

Como observa Silveira (2023, p. 89): "A digitalização de serviços essenciais sem adequadas salvaguardas de inclusão pode transformar a exclusão digital em exclusão de direitos fundamentais".

4.4.2 Concentração de Poder Econômico

A substituição do sistema atual de registros públicos por registros em blockchain operados por empresas privadas pode resultar em:

a) Oligopólio de provedores tecnológicos;
b) Captura regulatória por grandes empresas;
c) Subordinação do interesse público a interesses comerciais;
d) Monetização de dados pessoais e comportamentais.

5 AMEAÇAS DA COMPUTAÇÃO QUÂNTICA ÀS MOEDAS DIGITAIS

5.1 Panorama Atual do Desenvolvimento Quântico Global

A computação quântica deixou de ser uma possibilidade teórica e já se materializa em diversos países:

5.1.1 Principais Desenvolvimentos por País

a) **Estados Unidos**:
   - IBM: Processador Eagle de 127 qubits e Osprey de 433 qubits
   - Google: Demonstração de "supremacia quântica" com o processador Sycamore
   - Investimentos públicos e privados superiores a US$ 25 bilhões

b) **China**:
   - Processador Jiuzhang de 76 qubits fotônicos
   - Investimento governamental de US$ 10 bilhões no programa quântico nacional
   - Rede de comunicação quântica entre Pequim e Xangai

c) **União Europeia**:
   - Iniciativa Quantum Flagship com investimento de €1 bilhão
   - Desenvolvimento de computadores quânticos na Alemanha, França e Países Baixos
   - Foco em criptografia pós-quântica

d) **Outros países com programas avançados**:
   - Reino Unido, Canadá, Japão, Israel, Coreia do Sul e Austrália

5.1.2 Implicações do Desenvolvimento Assimétrico

O desenvolvimento desigual da tecnologia quântica cria assimetrias de poder significativas:

a) Vantagem estratégica para países pioneiros;
b) Potencial para vigilância econômica transnacional;
c) Vulnerabilidade de sistemas financeiros de países sem capacidade quântica;
d) Nova dimensão de segurança nacional.

5.2 Vulnerabilidades Criptográficas das CBDCs

5.2.1 Algoritmo de Shor e Criptografia Assimétrica

O algoritmo de Shor, quando implementado em computadores quânticos adequados, representa uma ameaça direta aos sistemas de criptografia de chave pública:

a) Fatoração eficiente de números grandes, comprometendo RSA

OBS: RSA é, na atualidade, um dos padrões mais confiáveis de criptografia assimétrica, que se utiliza de chaves públicas e privadas como forma de proteger informações armazenadas, utilizado para proteger e-mails, transações financeiras, sistemas de autenticação e assinaturas eletrônicas, por exemplo.

b) Solução do problema do logaritmo discreto, afetando a criptografia de curva elíptica (uma forma de criptografia de chave pública baseada na matemática das curvas elípticas, utilizada no algoritmo de assinatura digital conhecido como ECDSA);

c) Comprometimento potencial das assinaturas digitais utilizadas em blockchains.

Bernstein e Lange (2023, p. 45) estimam que "com aproximadamente 4.000 qubits lógicos estáveis, computadores quânticos poderão quebrar chaves RSA de 2048 bits em questão de horas, tornando inseguros os sistemas atuais de blockchain".

5.2.2 Algoritmo de Grover e Funções Hash

O algoritmo de Grover pode quadraticamente acelerar ataques a funções hash:

a) Redução significativa na segurança de algoritmos como SHA-256;
b) Necessidade de dobrar o tamanho das chaves para manter segurança equivalente;
c) Impacto potencial na mineração e validação de blockchains.

OBS: Sucintamente, a “mineração”é um processo fundamental para que moedas digitais sejam geradas e confiáveis. Envolve um procedimento importante para as moedas digitais serem geradas e confiáveis, visto que é através dele que são validados os blocos de transações nas redes blockchain.

5.2.3 Vulnerabilidades de Contratos Inteligentes

Contratos inteligentes baseados em criptografia atual tornam-se vulneráveis:

a) Comprometimento das assinaturas de autorização;
b) Possibilidade de falsificação de identidades digitais;
c) Riscos à integridade das transações automatizadas.

5.3 Estratégias de Mitigação: Criptografia Pós-Quântica

5.3.1 Desenvolvimento de Padrões Criptográficos Resistentes

Tenta-se desenvolver diversos algoritmos objetivando resistir a ataques quânticos:

a) **Criptografia baseada em reticulados** (CRYSTALS-Kyber, NTRU);
b) **Sistemas baseados em hash** (SPHINCS+);
c) **Códigos corretores de erros** (McEliece);

d) **Isogenias supersingulares** (SIKE, apesar das vulnerabilidades recentemente identificadas).

5.3.2 Desafios para Implementação em CBDCs

A transição para criptografia pós-quântica em CBDCs apresenta desafios significativos:

a) Maior complexidade computacional dos algoritmos pós-quânticos;
b) Desafios de interoperabilidade durante o período de transição;
c) Necessidade de sistemas de atualização contínua para acompanhar avanços em ataques;
d) Balanceamento entre segurança e eficiência operacional.

6 PROPOSTA DE INTEGRAÇÃO: PRESERVAÇÃO E MODERNIZAÇÃO DO SISTEMA REGISTRAL

6.1 Fundamentos da Proposta de Integração

A análise dos riscos apresentados sugere a necessidade de uma abordagem integrativa que preserve o sistema constitucional de registros públicos, incorporando-lhe inovações tecnológicas como o blockchain, tokenização de ativos, etc. Esta proposta baseia-se em três princípios fundamentais:

a) **Preservação constitucional**: manutenção da estrutura constitucional do sistema de registros públicos;

b) **Complementaridade tecnológica**: adoção de blockchain como camada complementar, não substitutiva;

c) **Redundância estratégica**: manutenção de sistemas paralelos como estratégia de segurança.

d) **Eliminação de conflitos**: estando ambos sistemas, com base em blockchain e tradicional, sob operação dos mesmos agentes, centralizados no SERP - Sistema Eletrônico dos Registros Públicos, elimina-se o risco de registros divergentes.

6.2 Estrutura do Sistema Integrado

6.2.1 Registradores Públicos como Validadores Primários

Neste modelo, os registradores públicos atuariam como validadores primários na rede blockchain do Drex:

a) Utilização da capilaridade nacional dos cartórios como nós da rede;
b) Aproveitamento da fé pública e da responsabilidade pessoal dos registradores;
c) Manutenção da qualificação jurídica prévia aos registros em blockchain;
d) Garantia da fundamental supervisão judicial sobre o sistema.

6.2.2 Tokenização com Segurança Jurídica

A tokenização de ativos reais (máquinas, imóveis, veículos, empresas, etc.) seria realizada mediante:

a) Verificação prévia da situação jurídica pelo registrador competente;
b) Registro simultâneo no sistema tradicional e na blockchain;
c) Vinculação permanente entre o registro tradicional e o token;
d) Possibilidade de intervenção judicial em ambos os sistemas.

6.2.3 Interoperabilidade com o Sistema Financeiro Nacional

O sistema integrado seria plenamente interoperável com o Banco Central e o Sistema Financeiro Nacional:

a) Acesso dos registradores a APIs do Sistema Financeiro;
b) Integração com o Sistema de Pagamentos Brasileiro (SPB);
c) Compatibilidade com o Pix e outros meios de pagamento;
d) Compartilhamento seguro de informações relevantes.

6.3 Vantagens do Modelo Integrado

6.3.1 Segurança Jurídica Reforçada

O modelo integrado fortalece a segurança jurídica ao:

a) Manter a base constitucional dos registros;
b) Aproveitar a jurisprudência consolidada;
c) Preservar mecanismos conhecidos de resolução de conflitos;
d) Garantir a supervisão e mesmo a intervenção judicial quando necessária.

6.3.2 Resiliência Tecnológica Ampliada

A redundância entre sistemas tradicional e blockchain proporciona:

a) Proteção contra ataques cibernéticos através da diversificação;
b) Mitigação dos riscos de ameaças quânticas;
c) Preservação de registros em caso de falhas em um dos sistemas;
d) Facilidade de auditoria e verificação cruzada.

6.3.3 Inclusão Digital Facilitada

O modelo híbrido facilita a inclusão ao:

a) Manter o atendimento presencial para populações com dificuldade de acesso digital;
b) Permitir a adoção gradual de novas tecnologias;
c) Fornecer orientação jurídica pelos registradores;
d) Garantir acesso universal independentemente da infraestrutura tecnológica disponível.

6.4 Desafios e Requisitos de Implementação

6.4.1 Adaptação Tecnológica do Sistema Registral

A implementação do modelo integrado exigiria:

a) Modernização tecnológica dos cartórios, o que já é uma realidade, que poderá ser melhorada;
b) Capacitação técnica dos registradores e funcionários;
c) Padronização nacional de protocolos e interfaces;
d) Investimento em infraestrutura de segurança.

6.4.2 Marco Regulatório Adequado

Seria necessário desenvolver:

a) Legislação específica para registros híbridos;
b) Regras claras sobre responsabilidade em cada sistema;
c) Protocolos de resolução de divergências entre registros;
d) Normas de interoperabilidade entre sistemas.

7 RECOMENDAÇÕES PARA POLÍTICAS PÚBLICAS

7.1 Recomendações Legislativas

7.1.1 Desenvolvimento de Marco Legal Específico

a) Elaboração de lei específica para CBDCs e tokenização de ativos;
b) Estabelecimento de regras de interação entre sistema registral e blockchain, no âmbito do SERP - Sistema Eletrônico dos Registros Públicos;
c) Definição clara de responsabilidades civis e penais;
d) Regulamentação da proteção de dados pessoais no contexto de CBDCs.

7.1.2 Atualização Normativa do Sistema Registral

a) Modernização da Lei de Registros Públicos (Lei 6.015/73), para contemplar os registros em blockchain, tokens e sua interação com o sistema tradicional, a ser mantido como redundância;
b) Adaptação da Lei dos Cartórios (Lei 8.935/94) para acomodar funções digitais;
c) Aprimoramento da legislação sobre assinaturas digitais e identidade digital;
d) Estabelecimento de padrões técnicos obrigatórios.

7.2 Recomendações para o Banco Central

7.2.1 Implementação Gradual e Segura do Drex

a) Adoção de abordagem gradual e baseada em evidências;
b) Realização de testes extensivos em ambientes controlados;
c) Inclusão dos registradores públicos de títulos e documentos e de imóveis, nos grupos de trabalho;
d) Desenvolvimento conjunto de protocolos de segurança.

7.2.2 Preparação para Ameaças Quânticas

a) Implementação proativa de criptografia pós-quântica;
b) Desenvolvimento de protocolos de migração;
c) Realização de testes de resistência quântica;
d) Cooperação internacional em segurança criptográfica.

7.3 Recomendações para o Poder Judiciário

7.3.1 Desenvolvimento de Competências Digitais

a) Capacitação de magistrados em tecnologia blockchain;
b) Criação de varas especializadas em conflitos digitais;
c) Estabelecimento de protocolos de execução de decisões em blockchain;
d) Desenvolvimento de jurisprudência sobre registros digitais.

7.3.2 Supervisão do Sistema Integrado

a) Adaptação dos mecanismos de fiscalização para o ambiente digital;
b) Desenvolvimento de ferramentas de auditoria para registros em blockchain;
c) Capacitação das corregedorias para supervisão tecnológica;
d) Estabelecimento de padrões de compliance digital.

7.4 Recomendações para a Segurança Nacional

7.4.1 Desenvolvimento de Capacidade Quântica Nacional

a) Investimento em pesquisa e desenvolvimento quântico;
b) Formação de recursos humanos especializados;
c) Parcerias internacionais estratégicas;
d) Criação de infraestrutura quântica brasileira.

7.4.2 Proteção de Infraestrutura Crítica

a) Classificação do sistema Drex como infraestrutura crítica nacional;
b) Desenvolvimento de protocolos de contingência;
c) Realização regular de testes de invasão e resiliência;
d) Estabelecimento de redundâncias geográficas e tecnológicas.

8 CONCLUSÃO

A implementação do Drex representa uma oportunidade significativa de modernização do sistema financeiro brasileiro, mas sua execução deve respeitar os fundamentos constitucionais do ordenamento jurídico nacional. O sistema brasileiro de registros públicos, previsto no artigo 236 da Constituição Federal, constitui pilar fundamental da segurança jurídica e deve ser integrado às novas tecnologias, nunca descartado.

A análise desenvolvida evidencia que um modelo híbrido, que preserve o sistema registral existente enquanto incorpora as vantagens da tecnologia blockchain como camada complementar, apresenta vantagens significativas em termos de segurança jurídica, resiliência tecnológica e inclusão social. Esta abordagem permite aproveitar o melhor de ambos os sistemas: a segurança jurídica e a fé pública do sistema tradicional, combinadas com a eficiência e transparência do blockchain.

Os desafios emergentes da computação quântica reforçam a necessidade de uma abordagem cautelosa e redundante, que não aposte todas as garantias em uma única tecnologia. A preservação do sistema tradicional de registros públicos como camada adicional de segurança

não representa duplicidade de custos, mas sim uma estratégia essencial de resiliência diante das incertezas tecnológicas futuras e não significará acréscimo de ônus para os usuários.

A modernização do sistema financeiro brasileiro através do Drex deve, portanto, ser construída sobre a base sólida do sistema constitucional existente, em um processo de evolução gradual que preserve conquistas históricas de segurança jurídica enquanto incorpora inovações tecnológicas. O futuro digital do Brasil não exige a ruptura com suas instituições fundamentais, mas sua evolução integrada às novas realidades tecnológicas.

REFERÊNCIAS

AYANDELE, I. The eNaira experiment: Lessons from Nigeria's central bank digital currency implementation. **Journal of African Economies**, v. 32, n. 2, p. 67-89, 2023.

BANCO CENTRAL DO BRASIL. **Diretrizes para implementação do Drex: relatório da fase de estudos**. Brasília: BCB, 2023.

BANK FOR INTERNATIONAL SETTLEMENTS. **Central bank digital currencies: foundations, functions and future**. BIS Papers, n. 145. Basel: BIS, 2023.

BERNSTEIN, D. J.; LANGE, T. Post-quantum cryptography for blockchain systems. **Journal of Cryptologic Research**, v. 7, n. 2, p. 34-56, 2023.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988.

DIP, R. **Segurança jurídica e sistema registral brasileiro**. São Paulo: Saraiva, 2022.

LAMANA PAIVA, J. P. A constitucionalidade do sistema registral brasileiro e os desafios da tokenização de ativos. **Revista de Direito Imobiliário**, v. 85, p. 102-125, 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Post-Quantum Cryptography Standardization**. Gaithersburg: NIST, 2022.

PEOPLE'S BANK OF CHINA. **Progress of Research & Development of E-CNY in China**. Beijing: PBoC, 2023.

SILVEIRA, S. A. Exclusão digital e direitos fundamentais no Brasil contemporâneo. **Revista Direito e Práxis**, v. 14, n. 2, p. 75-97, 2023.

Autor: Emílio Guerra, engenheiro químico pela UERJ, engenheiro econômico pela UFRJ, bacharel em direito pela UERJ, ex-advogado, especialista em registros públicos pela PUC-MG, foi oficial registrador de imóveis e atualmente é oficial registrador de títulos e documentos, do 1º Ofício de Registro de Títulos e Documentos de Belo Horizonte, e membro do Comitê Técnico do Operador Nacional de Registro de Títulos e Documentos e Civil de Pessoas Jurídicas, do SERP - Sistema Eletrônico dos Registros Públicos.

* Artigo elaborado com o auxílio de pesquisas por mecanismos de busca como google e inteligência artificial.