Blockchain Intelligence e Regulação dos Ativos Virtuais: rastreabilidade *on-chain*, SPSAVs e proteção do consumidor em perspectiva comparada com o *CLARITY Act*

DOI: https://doi.org/10.58766/rpgbcb.v20i1.1309

Jardel Jardelino de Lima*

Recebido/Received: 8/8/2026
Aprovado/Approved: 29/9/2026

Introdução. 1 Ativos virtuais, pseudonimidade e rastreabilidade. 2 O marco regulatório brasileiro e as SPSAVs. 2.1 Autorização, modalidades e integração ao sistema regulado. 2.2 Proteção do cliente, governança e controles. 3 Blockchain Intelligence *como infraestrutura de* compliance*. 3.1 Monitoramento e abordagem baseada em risco. 3.2 Limites das heurísticas e da atribuição de identidade. 4 Fraudes, proteção do consumidor e resposta investigativa. 5 Custódia, segregação e verificabilidade. 6 Evidência* on-chain *e cadeia de custódia. 7 O* CLARITY Act *e a experiência norte-americana. 7.1 Estrutura de mercado e delimitação regulatória. 7.2 Convergências e diferenças com o modelo brasileiro. 8 Regulação proporcional e concorrência. 9 Proposta metodológica para uso de* Blockchain Intelligence*. Conclusão.*

Resumo

O trabalho examina a *Blockchain Intelligence* como instrumento de *compliance*, proteção do consumidor e investigação no novo regime brasileiro de ativos virtuais. Objetiva avaliar em que medida a rastreabilidade de *blockchain*s públicas pode auxiliar sociedades prestadoras de serviços de ativos virtuais sem converter inferências analíticas em presunções automáticas de identidade ou responsabilidade. Adota método qualitativo, exploratório, jurídico-dogmático e comparado, com análise da Lei 14.478, de 21 de dezembro de 2022, da regulamentação do Banco Central do Brasil, dos padrões do GAFI/FATF e da evolução legislativa do *Digital Asset Market Clarity Act* nos Estados Unidos. Os resultados indicam que a institucionalização das SPSAVs aumenta a relevância de controles capazes de integrar dados cadastrais, monitoramento transacional e informações *on-chain*, especialmente na prevenção à lavagem de dinheiro, fraude, custódia e resposta a incidentes. Conclui que *Blockchain Intelligence* pode ampliar a transparência e a capacidade investigativa, desde que submetida a validação técnica, documentação metodológica, correlação com dados externos legítimos e classificação explícita do grau de certeza das inferências. Propõe-se, ao final, um modelo em cinco etapas para preservação, verificação, análise, correlação e classificação da evidência.

Palavras-chave: ativos virtuais; *blockchain intelligence*; SPSAV; *compliance*; proteção do consumidor; prova digital.

* Mestrando em Cyber Security pela AGTU - American Global Tech University, Perito judicial, com atuação especializada em computação forense, segurança da informação, crimes cibernéticos, investigação de fraudes eletrônicas e rastreamento de criptoativos. Desenvolve trabalhos relacionados à produção e análise de provas digitais, Blockchain Intelligence, investigação patrimonial e análise forense aplicada a demandas judiciais e extrajudiciais. https://orcid.org/0009-0001-4474-5712

Blockchain Intelligence and Virtual Asset Regulation: on-chain traceability, VASPs and consumer protection in comparative perspective with the Clarity Act

Abstract

This paper examines Blockchain Intelligence as an instrument for compliance, consumer protection and investigations under Brazil's new virtual-asset regulatory framework. It aims to assess how traceability on public blockchains may assist virtual asset service providers without turning analytical inferences into automatic assumptions of identity or liability. The study adopts a qualitative, exploratory, doctrinal and comparative method, analyzing Brazilian Law No. 14,478/2022, Banco Central do Brasil regulations, FATF standards and the legislative development of the Digital Asset Market Clarity Act in the United States. The findings indicate that the institutionalization of regulated virtual asset service providers increases the relevance of controls capable of integrating customer data, transaction monitoring and on-chain information, particularly for anti-money laundering, fraud prevention, custody and incident response. It concludes that Blockchain Intelligence may strengthen transparency and investigative capacity when supported by technical validation, methodological documentation, lawful correlation with external data and explicit classification of the degree of certainty of analytical inferences. Finally, a five-stage model is proposed for preservation, verification, analysis, correlation and evidence classification.

Keywords: *virtual assets; blockchain intelligence; VASP; compliance; consumer protection; digital evidence.*

Introdução

A expansão dos ativos virtuais deixou de constituir fenômeno periférico para integrar a agenda regulatória, prudencial e de proteção do consumidor. Redes públicas de *blockchain* permitem transferência de valor, execução de contratos inteligentes e formação de mercados que operam continuamente e, em muitos casos, atravessam fronteiras sem depender da mesma arquitetura institucional que caracteriza os sistemas financeiros tradicionais. Ao mesmo tempo, *exchanges*, custodiantes, corretoras, emissores e outros intermediários passaram a desempenhar funções economicamente semelhantes às de instituições já conhecidas pelo direito financeiro.

No Brasil, a Lei 14.478/2022 estabeleceu diretrizes para a prestação de serviços de ativos virtuais, definiu ativo virtual para os fins do marco legal e condicionou o funcionamento das prestadoras à prévia autorização do órgão ou entidade federal competente (Brasil, 2022). O Decreto 11.563/2023 atribuiu ao Banco Central do Brasil competência para regular a prestação desses serviços e autorizar e supervisionar as prestadoras, preservadas as competências da Comissão de Valores Mobiliários quanto aos valores mobiliários (Brasil, 2023). A regulamentação posterior do Banco Central transformou essa autorização legislativa em um regime institucional concreto.

A Resolução BCB 520/2025 disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais (SPSAVs) e a prestação desses serviços por outras instituições autorizadas. A norma classifica as SPSAVs, conforme os serviços prestados, em intermediárias, custodiantes e corretoras de ativos virtuais (Banco Central do Brasil, 2025a). Em paralelo, a Resolução BCB 519/2025 disciplina o processo de autorização, enquanto a Resolução BCB 521/2025 trata de hipóteses em que operações com

CC BY NC SA

ativos virtuais se inserem no mercado de câmbio e de capitais internacionais (Banco Central do Brasil, 2025b; 2025c).

Esse movimento regulatório modifica o problema jurídico. A questão já não consiste apenas em saber se o mercado de ativos virtuais deve ser regulado, mas em definir quais controles são adequados à sua infraestrutura tecnológica, quais riscos justificam intervenção, como preservar concorrência e inovação e de que maneira dados produzidos por *blockchain*s podem ser utilizados por agentes privados e autoridades sem extrapolar o que tecnicamente demonstram.

É nesse espaço que se insere a *Blockchain Intelligence*. A expressão é empregada neste artigo para designar o conjunto de métodos, processos e ferramentas destinados a coletar, organizar, correlacionar e interpretar dados de redes *blockchain* com o objetivo de compreender fluxos de ativos, padrões transacionais, interações com serviços e exposições relevantes. Trata-se de uma disciplina aplicada que pode apoiar *compliance*, prevenção à lavagem de dinheiro e ao financiamento do terrorismo, gestão de risco, resposta a incidentes e investigações.

O problema de pesquisa é o seguinte: em que medida a *Blockchain Intelligence* pode contribuir para o cumprimento das obrigações regulatórias, a prevenção de fraudes e a proteção do consumidor no regime brasileiro das SPSAVs sem transformar heurísticas e classificações analíticas em presunções automáticas de identidade, autoria ou responsabilidade? A hipótese sustentada é que sua utilidade aumenta à medida que os intermediários são institucionalizados, mas sua confiabilidade depende de metodologia documentada, validação dos fatos *on-chain* e correlação criteriosa com dados *off-chain*.

O trabalho adota metodologia qualitativa, exploratória, jurídico-dogmática e comparada. Analisa a Lei 14.478/2022, atos do Banco Central, padrões internacionais do GAFI/FATF, literatura institucional sobre riscos de intermediários de criptoativos e a evolução do *Digital Asset Market Clarity Act* (*CLARITY Act*) nos Estados Unidos. A comparação não pressupõe equivalência entre os sistemas. Seu objetivo é identificar convergências e diferenças na tentativa de combinar segurança jurídica, integridade de mercado, proteção do usuário e inovação.

1 Ativos virtuais, pseudonimidade e rastreabilidade

O caráter pseudônimo de muitas *blockchains* públicas é frequentemente confundido com anonimato absoluto. Em uma rede como Bitcoin, o registro público demonstra entradas, saídas, valores, referências temporais, identificadores de transação e relações entre unidades de valor, sem apresentar, por si só, o nome civil do controlador de cada endereço. O NIST observa que, no Bitcoin, os usuários podem operar de forma pseudônima, uma vez que os identificadores das contas e as transações permanecem visíveis no registro público sem que a criação do endereço dependa necessariamente de um processo de identificação do usuário (Yaga *et al.*, 2018). Em redes baseadas em contas, como Ethereum, também é possível observar endereços, transferências, chamadas a contratos e eventos registrados na cadeia.

Essa arquitetura cria uma distinção essencial entre **rastreabilidade transacional e atribuição de identidade**. A *blockchain* pode permitir a reconstrução objetiva de determinado percurso transacional, mas a atribuição de um endereço a uma pessoa física ou jurídica constitui operação epistemologicamente distinta. A primeira conclusão pode decorrer diretamente do registro distribuído; a segunda pode depender de dados cadastrais de uma prestadora, apreensão de dispositivo, informação fornecida por terceiro, análise de infraestrutura, declaração do próprio usuário ou heurísticas de atribuição. A literatura técnica sobre *blockchain* reforça essa distinção ao demonstrar que a publicidade e a persistência dos registros não eliminam

a pseudonimidade dos participantes nem transformam, automaticamente, identificadores criptográficos em identidades civis (Yaga *et al.*, 2018).

A permanência e a resistência à alteração dos registros constituem vantagens investigativas relevantes. O NIST caracteriza *blockchains* como registros digitais distribuídos resistentes à adulteração, nos quais transações publicadas são preservadas de modo a permitir sua posterior verificação (Yaga *et al.*, 2018). Uma transação confirmada, portanto, não desaparece simplesmente porque o agente altera posteriormente sua estratégia operacional. O histórico pode ser reanalisado quando novos elementos se tornam disponíveis. Essa propriedade favorece investigações retrospectivas e permite que informações obtidas posteriormente – por exemplo, a identificação legítima de uma carteira depositária de uma *exchange* – sejam correlacionadas com fluxos anteriores.

Contudo, transparência do registro não significa transparência integral do contexto ou da identidade. Uma transferência pode representar pagamento, movimentação entre carteiras do mesmo controlador, depósito em serviço custodial, execução automatizada, reorganização operacional ou outra finalidade. O dado *on-chain* demonstra o evento técnico registrado; sua interpretação econômica, investigativa ou jurídica depende de elementos adicionais. A literatura sobre mecanismos destinados a ampliar a privacidade no Bitcoin demonstra, ainda, que determinadas técnicas podem dificultar inferências baseadas exclusivamente no histórico transacional, reforçando a necessidade de cautela metodológica na atribuição de relações entre endereços e usuários (Möser; Böhme, 2017). Essa diferença entre observação, inferência e atribuição deve acompanhar toda análise de *Blockchain Intelligence*.

2 O marco regulatório brasileiro e as SPSAVs

A Lei 14.478/2022 inaugurou um marco geral baseado em autorização e supervisão. O art. 3º define ativo virtual como representação digital de valor que pode ser negociada ou transferida por meios eletrônicos e utilizada para pagamento ou investimento, excluindo, entre outros itens, moeda nacional, moedas estrangeiras, moeda eletrônica, certos instrumentos de fidelidade e representações de ativos já submetidas a disciplina legal ou regulamentar própria (Brasil, 2022). A lei também prevê aplicação, no que couber, do Código de Defesa do Consumidor às operações no mercado de ativos virtuais.

A regulamentação do Banco Central aprofunda essa estrutura. A Resolução BCB 520/2025 define as SPSAVs como instituições autorizadas a funcionar pelo Banco Central que executam, em nome de terceiros, serviços de ativos virtuais. A classificação em intermediárias, custodiantes e corretoras evidencia que o regulador não trata o setor como atividade homogênea, mas diferencia funções e combinações de serviços (Banco Central do Brasil, 2025a).

A institucionalização aproxima o mercado de ativos virtuais de padrões de governança e controle presentes no sistema financeiro. O Banco Central informou, ao divulgar as Resoluções 519, 520 e 521, que a regulação estende às entidades prestadoras de serviços de ativos virtuais regras sobre proteção e transparência nas relações com clientes, prevenção à lavagem de dinheiro e ao financiamento do terrorismo, governança, segurança, controles internos e prestação de informações (Banco Central do Brasil, 2025d).

Essa aproximação não significa que os riscos sejam idênticos aos de bancos. O Financial Stability Institute observa que grandes prestadores de serviços de criptoativos expandiram suas atividades para além de negociação e custódia, oferecendo produtos semelhantes a funções tradicionais de intermediação financeira. Quando assumem riscos de crédito, liquidez e maturidade, podem reproduzir vulnerabilidades conhecidas sem necessariamente possuir, em todas as jurisdições, salvaguardas prudenciais equivalentes (Ocampo; Goodrich; Lovicu, 2026).

CC BY NC SA

O desenho regulatório brasileiro, portanto, deve ser compreendido como tentativa de reduzir a assimetria entre a função econômica exercida e o nível de controle exigido. Isso é especialmente importante quando a prestadora mantém ativos de clientes, executa ordens, realiza conversões, intermedeia operações ou se conecta ao sistema de pagamentos e ao mercado de câmbio.

2.1 Autorização, modalidades e integração ao sistema regulado

A autorização de funcionamento cria um ponto de responsabilização institucional. A atividade deixa de ser observada apenas pelo prisma contratual entre usuário e plataforma e passa a integrar um regime de supervisão administrativa. Esse deslocamento favorece padronização de controles e permite que o regulador exija capacidade operacional compatível com os serviços efetivamente prestados.

A Resolução BCB 520/2025 também contém mecanismo de integração com o perímetro regulado. Seu art. 91 estabelece, a partir de 30 de outubro de 2026, vedação para que instituições financeiras, instituições de pagamento e outras instituições autorizadas pelo Banco Central realizem ou viabilizem operações no mercado de ativos virtuais com contrapartes prestadoras que não estejam autorizadas ou em processo de autorização no País, ressalvadas as hipóteses admitidas pela própria norma (Banco Central do Brasil, 2025a).

O dispositivo tem efeito competitivo e de integridade. Ao limitar a conectividade de prestadores não regularizados com instituições supervisionadas, aumenta o valor econômico da autorização e reduz a possibilidade de arbitragem baseada apenas na ausência de controles. Ao mesmo tempo, impõe desafios de transição e de proporcionalidade, sobretudo para empresas menores que precisam adaptar governança, tecnologia e capital humano.

2.2 Proteção do cliente, governança e controles

A proteção do cliente no mercado de ativos virtuais possui dimensão informacional, operacional e patrimonial. Informação adequada sobre riscos é necessária, mas insuficiente se a entidade não possuir controles para proteger chaves, registrar autorizações, responder a incidentes, separar funções críticas e monitorar operações. A confiança do usuário em um custodiante é, simultaneamente, jurídica e tecnológica.

A governança deve considerar características específicas da infraestrutura *blockchain*. A irreversibilidade prática de muitas transações, a operação contínua das redes, a possibilidade de transferências transfronteiriças e a interação com protocolos descentralizados exigem procedimentos que não podem ser meras reproduções de controles concebidos exclusivamente para transferências bancárias tradicionais.

Nesse contexto, a *Blockchain Intelligence* pode funcionar como camada complementar de controle. Ela não substitui KYC, registros internos, segregação de funções ou segurança cibernética; agrega informação sobre o comportamento transacional externo à instituição e sobre a trajetória de ativos antes e depois de sua interação com a prestadora.

3 *Blockchain Intelligence* como infraestrutura de *compliance*

Compliance em ativos virtuais exige integração de fontes. Uma prestadora conhece informações cadastrais, dispositivos, sessões, ordens, contas internas e histórico de relacionamento. A *blockchain*, por sua vez, oferece dados sobre movimentações que podem anteceder o ingresso dos ativos na plataforma

ou prosseguir após a retirada. A junção desses planos aumenta a capacidade de compreender risco sem eliminar a necessidade de interpretação humana.

O GAFI/FATF aplica sua Recomendação 15 aos ativos virtuais e aos VASPs e vem acompanhando periodicamente sua implementação internacional. Em seu ***Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs***, publicado em 16 de julho de 2026, o organismo registrou continuidade dos avanços na implementação da Recomendação 15, incluindo avaliações de risco, desenvolvimento de estruturas regulatórias, licenciamento ou registro de VASPs, implementação da *Travel Rule* e medidas de supervisão e *enforcement*. O relatório ressalta, contudo, que permanecem lacunas relevantes na transformação das avaliações de risco em medidas efetivas de mitigação, na operacionalização dos regimes de licenciamento ou registro, na identificação de pessoas e entidades que desempenham atividades de VASP e na efetividade da supervisão baseada em risco (FATF, 2026).

A atualização de 2026 é particularmente relevante para a *Blockchain Intelligence* porque identifica riscos emergentes e crescentes relacionados ao uso de ativos virtuais. Entre eles estão a crescente **industrialização de fraudes envolvendo ativos virtuais por organizações criminosas**, o uso indevido de ***stablecoins***, os riscos decorrentes de transações ***peer-to-peer* realizadas por meio de *unhosted wallets***, a atuação de VASPs offshore fora de estruturas efetivas de supervisão e os desafios relacionados a arranjos de **finanças descentralizadas – DeFi** (FATF, 2026). Esses fenômenos ampliam a importância de mecanismos capazes de observar fluxos transacionais e correlacioná-los, de maneira proporcional e metodologicamente controlada, com informações obtidas fora da *blockchain*.

A abordagem baseada em risco é especialmente adequada à *Blockchain Intelligence*. O objetivo não deve ser classificar qualquer interação com determinada categoria como ilícita, mas identificar sinais que, combinados com valor, frequência, contraparte, jurisdição, comportamento do cliente e outras circunstâncias, justifiquem diligência adicional. O valor analítico está na priorização e na contextualização, não na produção automática de culpa.

Entre as aplicações possíveis estão a triagem de endereços antes de depósitos ou retiradas, monitoramento de exposição a serviços classificados como de maior risco, identificação de padrões de dispersão ou consolidação, acompanhamento de fluxos relacionados a incidentes conhecidos, análise de conexões com *bridges* e protocolos e apoio a investigações internas.

A utilização responsável exige uma trilha de auditoria. A instituição deve ser capaz de explicar qual dado foi observado, em qual rede, em que momento, por qual ferramenta ou método, qual regra gerou o alerta, quais verificações posteriores foram realizadas e qual decisão humana resultou da análise. Sem esse registro, o sistema de monitoramento pode tornar-se opaco inclusive para a própria organização.

3.1 Monitoramento e abordagem baseada em risco

Uma arquitetura madura de monitoramento pode combinar três camadas. A primeira é objetiva: fatos diretamente verificáveis na *blockchain*, como *hash*, bloco, endereço, valor e contrato. A segunda é analítica: padrões, *clusters*, tipologias e classificações. A terceira é contextual: dados cadastrais, histórico de conta, justificativas econômicas, documentos e informações provenientes de fontes externas legítimas.

O risco de erro aumenta quando essas camadas são confundidas. Uma etiqueta atribuída por fornecedor não possui a mesma natureza probatória de um *hash* de transação. Um *cluster* inferido por heurística não equivale, automaticamente, a uma entidade juridicamente identificada. Um alerta de proximidade com endereço de risco não demonstra conhecimento ou participação do cliente na atividade subjacente.

CC BY NC SA

Por isso, decisões de maior impacto devem observar proporcionalidade e possibilidade de revisão. A automação pode identificar anomalias em escala, mas a decisão final precisa considerar contexto, qualidade da fonte e alternativas explicativas plausíveis.

3.2 Limites das heurísticas e da atribuição de identidade

Heurísticas são instrumentos relevantes para analisar redes complexas, mas seus resultados possuem natureza inferencial. A literatura especializada demonstra que técnicas de análise de *blockchain* podem explorar padrões transacionais para estabelecer relações prováveis entre endereços e atividades, mas tais inferências não devem ser confundidas com identificação civil automaticamente comprovada. A própria característica pseudônima do Bitcoin pressupõe a distinção entre identificadores publicamente observáveis e a identidade das pessoas que os controlam (Yaga *et al.*, 2018).

No Bitcoin, técnicas de agrupamento podem explorar padrões de gasto; em redes de contas, relações com contratos, depósitos e retiradas podem auxiliar no mapeamento de serviços. Contudo, carteiras compartilhadas, serviços custodiais, mecanismos voltados à privacidade, *coinjoins*, *bridges*, contratos inteligentes e mudanças de comportamento podem reduzir a confiabilidade de determinadas inferências. Estudos empíricos sobre mecanismos de anonimização no ecossistema Bitcoin demonstram a relevância dessas técnicas para a análise dos limites da inferência transacional, reforçando que o contexto técnico do fluxo precisa ser considerado antes da formulação de conclusões categóricas (Möser; Böhme, 2017).

O problema jurídico surge quando uma inferência técnica é convertida em afirmação categórica sem documentação do caminho lógico que a sustenta. A boa prática consiste em separar explicitamente aquilo que foi diretamente observado na *blockchain* daquilo que resulta de inferência analítica. Essa separação protege o usuário contra falsos positivos, fortalece a auditabilidade do *compliance* e aumenta a qualidade de eventual elemento probatório apresentado à autoridade administrativa ou judicial.

Essa cautela também é coerente com a abordagem baseada em risco defendida pelo GAFI/FATF. A avaliação de risco pressupõe análise contextual e adoção de medidas proporcionais, não a transformação automática de um indicador isolado em conclusão sobre identidade, autoria ou responsabilidade (FATF, 2026).

A atribuição de identidade deve, sempre que possível, ser corroborada por fonte independente. Dados cadastrais fornecidos por instituição, apreensão forense de dispositivo, elementos de autenticação, registros de acesso e outras evidências podem reforçar ou enfraquecer determinada hipótese. *Blockchain Intelligence* torna-se metodologicamente mais robusta quando funciona como parte de um mosaico probatório, e não como fonte isolada de certeza.

4 Fraudes, proteção do consumidor e resposta investigativa

O mercado de ativos virtuais é utilizado legitimamente por milhões de pessoas, mas também é explorado em golpes de investimento, falsas plataformas, *phishing*, comprometimento de credenciais, engenharia social, extorsão e outras fraudes. A Lei 14.478/2022 incorporou expressamente a preocupação com fraude envolvendo ativos virtuais e determinou a incidência, no que couber, do Código de Defesa do Consumidor (Brasil, 2022).

A proteção do consumidor não se limita ao momento anterior à contratação. Inclui desenho seguro do serviço, autenticação, comunicação clara, mecanismos de contestação, resposta a incidentes, preservação de registros e cooperação com autoridades. Quando um golpe resulta em transferência para *blockchain*

pública, a rapidez da resposta pode ser determinante para identificar pontos de saída e interação com entidades reguladas.

Blockchain Intelligence pode apoiar essa resposta ao reconstruir o fluxo e localizar momentos em que ativos entram em serviços centralizados. A identificação de um depósito em determinada prestadora não significa, por si só, que o beneficiário final esteja identificado publicamente, mas cria um ponto potencial de cooperação institucional sujeito aos instrumentos jurídicos cabíveis.

A permanência dos registros também permite reabrir hipóteses analíticas. Uma carteira inicialmente desconhecida pode ser posteriormente associada a serviço ou entidade. Assim, preservação adequada dos identificadores originais – *hashes*, endereços, rede, bloco, horário e evidências de contexto – possui valor mesmo quando a recuperação imediata do ativo não é possível.

É importante, porém, evitar promessas irreais de recuperação. Rastreabilidade e recuperabilidade são conceitos distintos. O fato de um fluxo ser tecnicamente visível não significa que exista autoridade jurisdicional, contraparte cooperante, saldo remanescente ou mecanismo jurídico capaz de restituir o valor.

5 Custódia, segregação e verificabilidade

Custódia é uma das áreas em que a convergência entre regulação e tecnologia se torna mais evidente. O usuário que entrega a uma prestadora o controle operacional de seus ativos passa a depender da governança de chaves, dos processos de autorização e da solvência e integridade da entidade. Eventos de mercado demonstraram que intermediários multifuncionais podem concentrar riscos e conflitos quando acumulam negociação, custódia, crédito e outras atividades (Bank for International Settlements, 2024).

A segregação patrimonial busca reduzir a confusão entre recursos próprios e de clientes, mas sua efetividade operacional depende de controles que permitam reconciliar obrigações internas com ativos efetivamente controlados. Em *blockchain*, parte dessa verificação pode ser apoiada por dados públicos, embora a simples visualização de saldo em endereços não demonstre integralmente passivos, ônus, acordos fora da cadeia ou disponibilidade jurídica dos ativos.

Modelos de prova de reservas ilustram essa limitação. Demonstrar controle de determinados ativos é informativo, mas não substitui demonstração completa de obrigações. A transparência *on-chain* deve ser combinada com contabilidade, auditoria, governança e controles de acesso. O mesmo raciocínio vale para segregação: a arquitetura de carteiras precisa corresponder à realidade jurídica e contábil da instituição.

A gestão de chaves é igualmente crítica. Carteiras quentes favorecem liquidez operacional, enquanto armazenamento frio pode reduzir exposição a ataques remotos. Políticas de múltiplas assinaturas, computação multipartidária, segregação de funções e limites de movimentação podem reduzir riscos, mas nenhuma tecnologia elimina a necessidade de governança e resposta a incidentes.

6 Evidência *on-chain* e cadeia de custódia

Quando informações provenientes de *blockchain* são utilizadas em investigação administrativa, procedimento de *compliance* ou processo judicial, a reprodutibilidade da análise torna-se central. A natureza pública de determinada *blockchain* não dispensa documentação metodológica. O caráter distribuído, verificável e resistente à adulteração do registro constitui característica da própria infraestrutura, mas não garante, por si só, a correção das interpretações produzidas a partir dos dados (Yaga *et al.*, 2018).

CC BY NC SA

É necessário registrar qual rede foi consultada, quais identificadores foram analisados, quais ferramentas foram utilizadas e quais transformações ou inferências foram aplicadas.

Uma metodologia de cadeia de custódia para evidência *on-chain* deve preservar, no mínimo, os identificadores primários da transação, a fonte de consulta, data e hora da coleta, registros das telas ou exportações relevantes, versões das ferramentas quando materialmente importantes e os passos analíticos que conduziram às conclusões. Se a análise utilizar base proprietária, o relatório deve distinguir o dado verificável publicamente da classificação fornecida pelo terceiro.

Essa distinção decorre da própria diferença entre o registro originário da *blockchain* e as interpretações posteriormente construídas sobre ele. O objetivo não é congelar uma análise que, por natureza, pode evoluir à medida que novos elementos se tornam disponíveis, mas permitir que outro profissional compreenda e, quando tecnicamente possível, reproduza o caminho realizado. Uma conclusão que dependa de informação externa não disponível deve declarar expressamente essa dependência.

Com base nessa necessidade de separação epistemológica, **propõe-se neste trabalho**, para fins de comunicação técnica, uma taxonomia composta por quatro categorias: **fato *on-chain*, inferência analítica, informação *off-chain* e conclusão investigativa**. A classificação constitui proposta metodológica do autor construída a partir da distinção, reconhecida na literatura técnica, entre os registros diretamente verificáveis na *blockchain* e as interpretações e correlações produzidas a partir deles (Yaga *et al.*, 2018).

Fato *on-chain* é o evento diretamente verificável na rede, como endereço, *hash*, bloco, valor, contrato ou registro transacional. **Inferência analítica** corresponde à interpretação derivada de padrões, heurísticas, agrupamentos, tipologias ou classificações. **Informação *off-chain*** é o dado obtido fora da *blockchain*, como registros cadastrais, logs, documentos, elementos provenientes de dispositivos, informações de prestadores de serviços ou outras fontes externas legítimas. **Conclusão investigativa** é a síntese resultante da correlação fundamentada entre as categorias anteriores.

A taxonomia proposta busca reduzir o risco de circularidade e de sobrevalorização probatória das inferências. Se uma ferramenta analítica classifica determinado endereço como pertencente a uma entidade, por exemplo, o relatório não deve apresentar essa etiqueta como se constituísse informação nativa da *blockchain*. Deve identificar a origem da classificação, seu caráter inferencial, o nível de confiança disponível e, quando possível, o elemento independente utilizado para corroborar a atribuição.

A distinção é especialmente importante porque a publicidade do registro transacional não elimina a pseudonimidade dos participantes. A literatura técnica demonstra que os identificadores de uma *blockchain* podem ser observáveis sem que isso corresponda, automaticamente, à identificação da pessoa que os controla (Yaga *et al.*, 2018). Desse modo, preservar a fronteira entre fato verificável, inferência, informação externa e conclusão constitui requisito metodológico para que a capacidade analítica da *Blockchain Intelligence* não seja confundida com certeza probatória absoluta.

7 O *CLARITY Act* e a experiência norte-americana

Nos Estados Unidos, o debate sobre estrutura de mercado de ativos digitais ganhou forma no H.R. 3633, *Digital Asset Market Clarity Act of 2025*. A Câmara dos Representantes aprovou o projeto em 17 de julho de 2025 por votação bipartidária de 294 a 134. Em 14 de maio de 2026, o Senate Committee on Banking, Housing, and Urban Affairs aprovou, por 15 votos a 9, o avanço de uma versão do projeto, encaminhando-o ao plenário do Senado (U.S. House Committee on Financial Services, 2025; U.S. Senate Committee on Banking, Housing, and Urban Affairs, 2026a).

A experiência norte-americana é relevante porque procura reduzir incerteza sobre classificação de ativos, registro de intermediários e repartição de competências. O texto aprovado na Câmara contém definições e regras para *digital commodities*, prevê registro de *exchanges*, *brokers* e *dealers* e trata da aplicação do *Bank Secrecy Act*, entre outros temas (United States, 2025). A versão trabalhada no Senado também busca estabelecer salvaguardas e regras de mercado, embora o processo legislativo permaneça sujeito a alterações.

O *CLARITY Act* deve ser analisado como legislação em tramitação, e não como direito vigente consolidado. Essa cautela é particularmente importante em estudo comparado, pois versões legislativas podem modificar conceitos, competências e obrigações. O valor analítico do projeto está em revelar as escolhas regulatórias debatidas, não em atribuir-lhe efeitos jurídicos ainda inexistentes.

O discurso institucional favorável ao projeto enfatiza proteção de consumidores, combate a finanças ilícitas, segurança nacional e inovação responsável. Há também críticas no próprio Senado quanto à suficiência das salvaguardas e aos riscos para consumidores e para o sistema financeiro. Essa divergência confirma que clareza regulatória não é conceito unidimensional: regras claras podem ser mais ou menos protetivas, proporcionais ou competitivas conforme seu conteúdo (U.S. Senate Committee on Banking, Housing, and Urban Affairs, 2026b; 2026c).

7.1 Estrutura de mercado e delimitação regulatória

A fragmentação regulatória norte-americana é distinta da arquitetura brasileira. Nos Estados Unidos, parte central do debate envolve a fronteira entre a Securities and Exchange Commission e a Commodity Futures Trading Commission, além do tratamento jurídico de ativos que podem ter sido distribuídos em contextos associados a contratos de investimento e posteriormente negociados em mercados secundários.

No Brasil, a Lei 14.478/2022 exclui de seu regime os ativos representativos de valores mobiliários submetidos à Lei 6.385/1976 e preserva as competências da CVM. O Banco Central recebeu competência para regular, autorizar e supervisionar as prestadoras no âmbito definido pelo marco legal e pelo Decreto 11.563/2023. Assim, embora ambos os países busquem reduzir incerteza, partem de desenhos institucionais diferentes.

A comparação revela um ponto comum: a necessidade de definir o perímetro. Sem clareza sobre quais atividades estão sujeitas a autorização e qual autoridade supervisiona cada função, aumenta a arbitragem regulatória e diminui a previsibilidade para consumidores e empresas.

7.2 Convergências e diferenças com o modelo brasileiro

Há convergência na tentativa de trazer intermediários de ativos digitais para estruturas formais de registro, supervisão, transparência e prevenção a ilícitos. Também existe preocupação comum em preservar inovação e evitar que a regulação seja tão incerta ou onerosa que desloque atividades para ambientes menos supervisionados.

A diferença principal está no estágio e na técnica normativa. O Brasil já possui lei-quadro, decreto de competência e regulamentação específica do Banco Central em vigor para SPSAVs. O *CLARITY Act*, na data considerada neste trabalho, ainda integra processo legislativo norte-americano. A comparação, portanto, é entre um regime brasileiro em implementação e uma proposta norte-americana de estrutura de mercado em evolução.

CC BY NC SA

Para *Blockchain Intelligence*, a convergência é mais relevante do que a diferença institucional. Em ambos os ambientes, intermediários regulados precisam compreender a origem, o destino e o risco das transações que processam. Quanto mais clara a responsabilidade do intermediário, maior a necessidade de ferramentas capazes de interpretar a infraestrutura tecnológica na qual o ativo circula.

8 Regulação proporcional e concorrência

A institucionalização das SPSAVs aumenta custos de entrada. Governança, controles internos, segurança cibernética, *compliance*, auditoria, capital humano e infraestrutura tecnológica exigem investimento. Grandes bancos e grupos financeiros podem aproveitar estruturas preexistentes, enquanto empresas nativas de cripto de menor porte precisam construir parte relevante desses mecanismos.

Esse efeito não torna a regulação indesejável, mas exige proporcionalidade. Requisitos muito baixos podem transferir risco ao consumidor e incentivar modelos frágeis; requisitos excessivos podem concentrar o mercado e reduzir competição. O desenho eficiente deve relacionar intensidade regulatória à natureza, escala, complexidade e risco das atividades.

Também é necessário evitar a falsa dicotomia entre finanças centralizadas e descentralizadas. O BIS observa que DeFi busca reproduzir funções financeiras por meio de contratos inteligentes, mas apresenta vulnerabilidades próprias, como fragilidades operacionais, alavancagem, interconexão e descasamentos de liquidez (Bank for International Settlements, 2023). A existência de protocolos descentralizados não elimina a relevância de intermediários regulados; modifica a fronteira de interação entre usuários, código e instituições.

A competição futura pode ocorrer entre bancos, SPSAVs especializadas, infraestruturas descentralizadas e modelos híbridos. Nesse cenário, *Blockchain Intelligence* tende a tornar-se competência transversal: bancos que operem ativos virtuais, prestadoras especializadas e autoridades precisarão compreender fluxos *on-chain*, ainda que seus modelos de negócio sejam distintos.

A proporcionalidade também deve alcançar o uso de ferramentas analíticas. Bloqueios, encerramentos de relacionamento ou comunicações baseadas em risco não devem depender de uma única etiqueta sem validação. Quanto maior o impacto da decisão sobre o usuário, maior deve ser a exigência de revisão, fundamentação e documentação.

9 Proposta metodológica para uso de *Blockchain Intelligence*

Com base nos problemas identificados, propõe-se um modelo metodológico em cinco etapas aplicável a *compliance*, resposta a incidentes e investigações envolvendo ativos virtuais. O modelo não pretende substituir procedimentos legais ou políticas específicas de cada instituição; busca oferecer uma estrutura mínima para aumentar rastreabilidade metodológica e reduzir confusão entre fatos e inferências.

A primeira etapa é a preservação. Devem ser registrados os identificadores originais: *blockchain*, endereço, *hash* da transação, bloco, data e hora, ativo, valor, contrato quando aplicável e fonte inicial da informação. Evidências externas relevantes devem ser preservadas de modo compatível com sua natureza, mantendo-se registro de origem e integridade.

A segunda etapa é a verificação *on-chain*. Antes de aceitar a saída de uma ferramenta analítica, o profissional deve confirmar os fatos fundamentais em explorador confiável ou, quando necessário, por consulta direta à infraestrutura da rede. O objetivo é separar dado nativo de interpretação produzida por terceiros.

A terceira etapa é a análise. Nessa fase são examinados fluxos, *clusters*, exposição, tipologias, interações com serviços, *bridges*, contratos e demais padrões. Cada heurística relevante deve ser identificada. Quando uma classificação vier de fornecedor, a origem dessa classificação deve constar do registro técnico.

A quarta etapa é a correlação. Dados *on-chain* são comparados com informações *off-chain* obtidas legitimamente: cadastro, ordens, logs, documentos, registros de acesso, informações de contraparte, elementos de investigação ou fontes públicas. A correlação pode aumentar ou reduzir a força de uma hipótese.

A quinta etapa é a classificação da evidência e da conclusão. Recomenda-se marcar cada afirmação relevante como fato *on-chain*, inferência analítica, informação *off-chain* ou conclusão investigativa. Adicionalmente, quando a natureza do caso permitir, pode-se registrar grau de confiança e hipóteses alternativas.

O modelo possui duas vantagens. Primeiro, facilita auditoria interna e revisão por terceiro. Segundo, reduz o risco de que a linguagem de um relatório atribua certeza superior àquela permitida pelos dados. Em ambiente regulado, essa transparência é útil tanto para proteger o consumidor quanto para demonstrar diligência da instituição.

A proposta também favorece interoperabilidade entre *compliance* e perícia. Um alerta interno bem documentado pode, se necessário e juridicamente autorizado, ser compreendido por investigadores externos sem que seja preciso reconstruir integralmente o raciocínio inicial. Da mesma forma, uma investigação pode devolver à área de *compliance* tipologias mais precisas para aperfeiçoar controles futuros.

Conclusão

A regulação brasileira dos ativos virtuais entrou em etapa de institucionalização. A Lei 14.478/2022 estabeleceu o marco geral; o Decreto 11.563/2023 definiu a competência do Banco Central; e as Resoluções BCB 519, 520 e 521 estruturaram autorização, funcionamento e aspectos cambiais das prestadoras. A consequência é a formação de um perímetro regulado no qual intermediários precisam combinar governança financeira com compreensão técnica das redes em que os ativos circulam.

A pesquisa confirmou a hipótese de que *Blockchain Intelligence* pode desempenhar papel relevante nesse novo ambiente. Sua utilidade decorre da possibilidade de observar fluxos, reconstruir trajetórias, identificar pontos de interação com serviços e produzir sinais de risco que complementam dados cadastrais e registros internos. Isso é especialmente importante para prevenção à lavagem de dinheiro, fraude, custódia, resposta a incidentes e cooperação investigativa.

A mesma pesquisa demonstrou, contudo, que rastreabilidade não equivale a identidade. Um endereço não é uma pessoa; um *cluster* não é, por si só, prova de titularidade; uma etiqueta de risco não demonstra automaticamente conhecimento ou dolo; e a proximidade transacional com atividade ilícita não substitui análise de contexto. A confiabilidade da *Blockchain Intelligence* depende de documentação metodológica e de separação entre fato, inferência, informação externa e conclusão.

O estudo comparado com o *CLARITY Act* mostra que Brasil e Estados Unidos, apesar de arquiteturas distintas, enfrentam problema comum: criar um perímetro suficientemente claro para proteger usuários e a integridade do mercado sem impedir inovação. O Brasil encontra-se em fase de implementação de regras específicas para SPSAVs; o projeto norte-americano permanece em processo legislativo, ainda sujeito a modificações.

O equilíbrio regulatório também possui dimensão concorrencial. A imposição de controles aumenta custos, mas a ausência de controles pode socializar perdas e comprometer confiança. A resposta adequada não é escolher entre regulação e inovação, e sim construir requisitos proporcionais ao risco e tecnicamente aderentes às características dos ativos virtuais.

CC BY NC SA

A proposta metodológica em cinco etapas – preservação, verificação, análise, correlação e classificação – oferece um caminho para integrar *Blockchain Intelligence* ao *compliance* sem transformar automação em presunção. Ao tornar explícita a origem e a força de cada afirmação, a instituição melhora a qualidade de sua decisão e a auditabilidade do processo.

Conclui-se que a *Blockchain Intelligence* pode constituir uma ponte entre descentralização tecnológica e supervisão institucional. Seu valor não está em prometer transparência absoluta, mas em transformar registros públicos e persistentes em informação tecnicamente verificável, juridicamente contextualizada e metodologicamente responsável. Nesse sentido, a maturidade do mercado de ativos virtuais dependerá tanto de regras claras quanto da capacidade de interpretar corretamente a tecnologia que essas regras pretendem alcançar.

Referências

BANCO CENTRAL DO BRASIL. **Resolução BCB 519, de 10 de novembro de 2025**. Disciplina os processos de autorização relacionados às sociedades prestadoras de serviços de ativos virtuais. Brasília, DF: Banco Central do Brasil, 2025b. Disponível em: https://www.bcb.gov.br. Acesso em: 8 ago. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB 520, de 10 de novembro de 2025**. Disciplina a constituição e o funcionamento das sociedades prestadoras de serviços de ativos virtuais e a prestação de serviços de ativos virtuais por outras instituições autorizadas a funcionar pelo Banco Central do Brasil. Brasília, DF: Banco Central do Brasil, 2025a. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=520&tipo=Resolu%C3%A7%C3%A3o+BCB. Acesso em: 8 ago. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB 521, de 10 de novembro de 2025**. Disciplina operações com ativos virtuais relacionadas ao mercado de câmbio e capitais internacionais. Brasília, DF: Banco Central do Brasil, 2025c. Disponível em: https://www.bcb.gov.br. Acesso em: 8 ago. 2026.

BANCO CENTRAL DO BRASIL. **Banco Central regulamenta o uso de ativos virtuais e o funcionamento e a autorização das instituições que atuam nesse mercado**. Brasília, DF, 10 nov. 2025d. Disponível em: https://www.bcb.gov.br/detalhenoticia/20918/nota. Acesso em: 8 ago. 2026.

BANK FOR INTERNATIONAL SETTLEMENTS. **The financial stability implications of multifunction cryptoasset intermediaries**: executive summary. Basel: BIS, 2024. Disponível em: https://www.bis.org/fsi/fsisummaries/exsum_22202.htm. Acesso em: 8 ago. 2026.

BANK FOR INTERNATIONAL SETTLEMENTS. **The financial stability risks of decentralised finance**: executive summary. Basel: BIS, 2023. Disponível em: https://www.bis.org/fsi/fsisummaries/defi.htm. Acesso em: 8 ago. 2026.

BRASIL. **Decreto 11.563, de 13 de junho de 2023**. Regulamenta a Lei 14.478, de 21 de dezembro de 2022, para estabelecer competências ao Banco Central do Brasil. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br. Acesso em: 8 ago. 2026.

BRASIL. **Lei 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação das prestadoras de serviços de ativos virtuais. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Acesso em: 8 ago. 2026.

FINANCIAL ACTION TASK FORCE. **Virtual Assets**: Targeted Update on Implementation of the FATF Standards on VAs and VASPs. Paris: FATF/OECD, 2025. Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html. Acesso em: 8 ago. 2026.

NAKAMOTO, Satoshi. **Bitcoin**: A Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 8 ago. 2026.

OCAMPO, Denise Garcia; GOODRICH, Peter; LOVICU, Gian-Piero. **Cryptoasset service providers as financial intermediaries**: risks and policy approaches. FSI Occasional Papers, n. 27. Basel: Bank for International Settlements, 2026. Disponível em: https://www.bis.org/fsi/fsipapers27.htm. Acesso em: 8 ago. 2026.

UNITED STATES. House of Representatives. **H.R. 3633 – Digital Asset Market Clarity Act of 2025.** Rules Committee Print 119-6. Washington, DC, 2025. Disponível em: https://rules.house.gov/bill/119/hr-3633. Acesso em: 8 ago. 2026.

U.S. HOUSE COMMITTEE ON FINANCIAL SERVICES. **Financial Services Highlights Support for CLARITY Act.** Washington, DC, 18 jul. 2025. Disponível em: https://financialservices.house.gov/news/documentsingle.aspx?documentid=410816. Acesso em: 8 ago. 2026.

U.S. SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS. **Chairman Scott, Senate Banking Committee Advance Clarity Act in Historic Bipartisan Vote.** Washington, DC, 14 maio 2026a. Disponível em: https://www.banking.senate.gov/newsroom/majority/chairman-scott-senate-banking-committee-advance-clarity-act-in-historic-bipartisan-vote. Acesso em: 8 ago. 2026.

U.S. SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS. **The Facts**: The CLARITY Act Protects Main Street, Unleashes Responsible Innovation, and Cracks Down on Fraud and Money Laundering. Washington, DC, 12 maio 2026b. Disponível em: https://www.banking.senate.gov/newsroom/majority/the-facts-the-clarity-act-protects-main-street-unleashes-responsible-innovation-and-cracks-down-on-fraud-and-money-laundering. Acesso em: 8 ago. 2026.

U.S. SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS. **Senator Warren Opening Remarks at Committee Mark Up of the Clarity Act.** Washington, DC, 14 maio 2026c. Disponível em: https://www.banking.senate.gov/newsroom/minority/senator-warren-opening-remarks-at-committee-mark-up-of-the-clarity-act. Acesso em: 8 ago. 2026.

FINANCIAL ACTION TASK FORCE. **Seventh Targeted Update on Implementation of the FATF Standards on Virtual Assets/VASPs**. Paris: FATF/OECD, 2026. Disponível em: FATF – Seventh Targeted Update 2026. Acesso em: 17 set. 2026.

MÖSER, Malte; BÖHME, Rainer. **The price of anonymity**: empirical evidence from a market for Bitcoin anonymization. **Journal of Cybersecurity**, v. 3, n. 2, p. 127–135, 2017. DOI: 10.1093/cybsec/tyx007. Disponível em: Oxford Academic – The price of anonymity. Acesso em: 17 set. 2026.

CC BY NC SA

YAGA, Dylan; MELL, Peter; ROBY, Nik; SCARFONE, Karen. ***Blockchain* Technology Overview.** NISTIR 8202. Gaithersburg, MD: National Institute of Standards and Technology, 2018. DOI: 10.6028/NIST.IR.8202. Disponível em: NIST – *Blockchain* Technology Overview. Acesso em: 17 set. 2026.