BITCOIN COMO MEIO DE PAGAMENTO NO BRASIL: UMA ANÁLISE DA VIABILIDADE, EXECUÇÃO E REGULAMENTAÇÃO

Felippe dos Santos Giassi
felippe-giassi@hotmail.com
Graduando em Administração de Empresas
Prof. Dr. Abel Corrêa de Souza
Universidade do Extremo Sul Catarinense - UNESC

RESUMO

Esta pesquisa analisou a viabilidade do *Bitcoin* como meio de pagamento no Brasil sob as perspectivas teórica, técnica e regulatória. A fundamentação teórica apoiou-se na Escola Austríaca de Economia, com ênfase nas obras de Mises, Hayek e Rothbard, complementada pela perspectiva liberal e pela Teoria dos Jogos aplicada à segurança da rede. A pesquisa caracterizou-se como exploratória, de natureza qualitativa, com procedimento bibliográfico, utilizando a análise de conteúdo como técnica de interpretação. Os resultados revelaram que o *Bitcoin* satisfaz os critérios monetários austríacos e que a *Lightning Network* resolve os gargalos técnicos da rede base, tornando-o competitivo com o PIX para pagamentos de baixo valor e superior para remessas transfronteiriças. O cenário regulatório mostrou-se o principal condicionante: a classificação do *Bitcoin* como ativo alienável pela Instrução Normativa RFB nº 1.888/2019 transforma cada transação em evento tributável, impondo um atrito fiscal que a moeda fiduciária não carrega. O Marco Legal dos Criptoativos e as Resoluções BCB nº 519, 520 e 521 legitimaram o setor, mas reproduziram nos pontos de acesso ao ecossistema os padrões institucionais do sistema financeiro tradicional. Concluiu-se que o *Bitcoin* é viável como meio de pagamento em contextos específicos; contudo, no cenário atual, é mais recomendável utilizá-lo como reserva de valor de longo prazo protegendo o patrimônio da inflação, enquanto a moeda fiduciária, por ser moeda fraca de uso corrente, permanece mais adequada para as transações cotidianas, conforme evidencia a Lei de Gresham.

Palavras-chave: *Bitcoin*. Meio de Pagamento. Escola Austríaca. Criptoativos. Regulação Brasileira

1 INTRODUÇÃO

O surgimento do *Bitcoin*, precursor e principal expoente dos criptoativos, não pode ser desassociado da crise financeira global de 2008, um evento que abalou a confiança no sistema bancário tradicional e nas políticas monetárias discricionárias. Apenas um mês após a quebra do banco de investimentos Lehman Brothers, um programador sob o pseudônimo de Satoshi Nakamoto publicou, em 31 de outubro de 2008, o artigo seminal "*Bitcoin*: um Sistema de Dinheiro Eletrônico *Peer-to-Peer*". A proposta era revolucionária: criar um sistema de pagamento que dispensasse a necessidade de um intermediário fiduciário, baseando-se "em prova criptográfica em vez de confiança" (Nakamoto, 2008).

A motivação de Nakamoto tornou-se explícita em 3 de janeiro de 2009, com a criação do primeiro bloco da rede *Bitcoin*, o "bloco gênese", que continha uma mensagem de texto com a manchete do jornal The Times daquele dia: "*Chancellor on brink of second bailout for banks*" (Chanceler à beira do segundo resgate aos bancos). Essa mensagem é um claro indicativo da visão crítica de seu criador sobre a instabilidade gerada pela intervenção estatal e pelo sistema bancário de reservas fracionárias (Ulrich, 2014).

Essa proposta tecnológica dialoga diretamente com uma longa tradição de pensamento econômico que questiona o monopólio estatal sobre a moeda. Carl Menger, fundador da Escola Austríaca, já havia estabelecido que "a moeda não foi gerada pela lei. Na sua origem, ela é uma instituição social, não estatal" (Menger, 1892). Seus sucessores, como Ludwig von Mises e Friedrich A. Hayek, aprofundaram essa crítica, argumentando que o controle governamental era a principal fonte de instabilidade econômica e inflação (Mises, 1953; Hayek, 2011).

O próprio Nakamoto sintetizou o problema ao afirmar que "o problema básico com a moeda convencional é toda a confiança necessária para fazê-la funcionar. Precisamos confiar que o banco central não desvalorizará o dinheiro, mas a história das moedas fiduciárias está repleta de quebras dessa confiança" (Ulrich, 2014.p. 106). Como observa Jeffrey Tucker (2014), o surgimento do *Bitcoin* representa uma reforma monetária "de fora para dentro e de baixo para cima, baseado nos princípios do empreendedorismo e das trocas de mercado", em um processo que se conforma ao modelo de Menger sobre a origem do dinheiro. No Brasil, um país com um histórico de instabilidade monetária, a discussão sobre a adoção de moedas digitais descentralizadas ganha contornos particulares.

A situação-problema que norteia esta pesquisa reside na aparente contradição entre a crescente adoção do *Bitcoin* como ativo de investimento por milhões de brasileiros e os persistentes obstáculos que impedem sua consolidação como um meio de pagamento cotidiano. Enquanto a tecnologia promete transações de baixo custo, sem intermediários e com uma política monetária previsível (Nakamoto, 2008; Ulrich, 2014), sua alta volatilidade, a concorrência com soluções estatais eficientes e um cenário regulatório em consolidação criam um ambiente de incerteza sobre sua função monetária primária.

A lacuna na pesquisa, portanto, está na falta de uma análise integrada que confronte a promessa teórica do *Bitcoin* como um "sistema de dinheiro eletrônico *peer-to-peer*" com a realidade prática, competitiva e regulatória do Brasil. Existe uma desconexão entre o potencial disruptivo da tecnologia e sua efetiva função monetária no cenário nacional, o que justifica uma investigação aprofundada sobre sua real viabilidade como meio de pagamento.

A crescente relevância dos criptoativos e a necessidade de compreender seu potencial e seus desafios em uma das maiores economias da América Latina, são elementos que justificam a realização do estudo. Nesse sentido, o trabalho apresenta como contribuições tanto teóricas, ao sintetizar a aplicação de teorias monetárias clássicas a um fenômeno digital, quanto práticas, ao oferecer a gestores, investidores e formuladores de políticas públicas uma análise integrada dos fatores que influenciam a adoção do *Bitcoin* no país.

Diante do exposto, a presente pesquisa busca responder à seguinte pergunta: Qual a viabilidade, sob as óticas de execução, base teórica e regulatória, do *Bitcoin* como meio de pagamento no Brasil? Neste alinhamento, o estudo tem por objetivo geral “Analisar a viabilidade do *Bitcoin* como meio de pagamento no contexto brasileiro sob as perspectivas teórica, técnica e regulatória”, sustentando-se em quatro objetivos específicos: (1) Expor a teoria da Escola Austríaca sobre a natureza da moeda como base analítica; (2) Analisar o protocolo *Bitcoin* como uma solução tecnológica para a desestatização do dinheiro; (3) Comparar a execução de pagamentos via *Bitcoin (Lightning Network)* e (4) Examinar o cenário jurídico-regulatório brasileiro para criptoativos.

O artigo foi estruturado em cinco seções. A primeira, esta introdução, contextualiza o problema de pesquisa. A segunda seção aprofunda a fundamentação teórica, explorando a inovação tecnológica do *blockchain*, as perspectivas da Escola Austríaca sobre a natureza da moeda e o cenário regulatório brasileiro. A terceira seção detalha os procedimentos metodológicos adotados. A quarta seção apresenta e discute os resultados da pesquisa, analisando o ecossistema de pagamentos, os desafios práticos à adoção e um estudo comparativo com outros sistemas de pagamento. Por fim, as considerações finais sintetizam os

achados, destacam as contribuições e limitações do estudo e propõem caminhos para futuras investigações.

2 FUNDAMENTAÇÃO TEÓRICA

A análise da viabilidade do *Bitcoin* como meio de pagamento exige uma imersão em três áreas interconectadas que se influenciam mutuamente: as seculares teorias econômicas sobre a natureza da moeda que esta tecnologia desafia, a sua revolucionária arquitetura tecnológica, e o complexo ambiente jurídico que surge como reação do Estado a este fenómeno. Esta seção explora esses três pilares de forma aprofundada, detalhando não apenas os seus conceitos, mas as suas implicações diretas para a função monetária do *Bitcoin*, construindo assim a base conceitual sobre a qual a discussão dos resultados será edificada.

2.1 A MOEDA E O SISTEMA MONETÁRIO

Para compreender a viabilidade do *Bitcoin*, é essencial analisar a natureza da moeda e a evolução dos sistemas de pagamento.

2.1.1 História e tipos de moeda

Smith (1996) argumenta que, uma vez estabelecida a divisão do trabalho, toda a sociedade se torna comercial, e cada homem vive da troca. No entanto, a troca direta, ou escambo, é dificultada pela necessidade de uma "dupla coincidência de desejos".

Smith (1996, p. 84-85) ilustra vividamente esse problema:

> O açougueiro tem mais carne em sua loja do que ele mesmo pode consumir, e o cervejeiro e o padeiro estariam dispostos, cada um, a comprar uma parte dela. Mas eles não têm nada a oferecer em troca, exceto os diferentes produtos de seus respectivos ofícios, e o açougueiro já está abastecido de toda a cerveja e pão de que necessita para o futuro imediato. Nesse caso, não pode haver troca entre eles. [...] A fim de evitar os inconvenientes dessa situação, todo homem prudente, em qualquer período da sociedade, após o primeiro estabelecimento da divisão do trabalho, deve ter-se empenhado naturalmente em gerir seus negócios de tal maneira que tivesse a qualquer momento em seu poder, além do produto específico de sua própria indústria, uma certa quantidade de alguma outra mercadoria, que ele imaginava que poucas pessoas recusariam em troca do produto de sua indústria.

Esse processo evolutivo, no qual o mercado converge para um meio de troca comum, demonstra que a moeda é uma instituição de origem espontânea (Menger, 1892).

Historicamente, diversas mercadorias serviram como meio de troca, mas os metais preciosos, como ouro e prata, prevaleceram como moeda-mercadoria por possuírem valor intrínseco e qualidades superiores como durabilidade, divisibilidade, portabilidade e escassez (Rothbard, 2013). Em contraste, a moeda-fiduciária (*fiat money*) não possui valor intrínseco; seu valor deriva exclusivamente da confiança e da imposição legal do governo por meio do curso forçado (Huerta De Soto, 2012). O sistema moderno é predominantemente fiduciário, uma evolução que, para a Escola Austríaca, representa uma degeneração da moeda de mercado para uma ferramenta de controle estatal (Rothbard, 2013).

2.1.2 Funções e características da moeda

Do ponto de vista da Escola Austríaca, a função essencial e definidora da moeda é a de ser um meio de troca universalmente aceito. Ludwig von Mises (1953) argumenta que esta é a sua função primária e essencial, da qual derivam as suas outras funções secundárias. A primeira função secundária é a de unidade de conta, que proporciona uma medida comum para expressar os preços de todos os outros bens e serviços, tornando o cálculo econômico possível. A segunda é a de reserva de valor, que permite a transferência de poder de compra ao longo do tempo (Rothbard, 2013).

O mercado, num contínuo processo de descoberta, seleciona como moeda a mercadoria que mais eficazmente encarna as propriedades de durabilidade, portabilidade, divisibilidade, fungibilidade e escassez. Esta emergência não é um ato arbitrário, mas o resultado de inúmeras ações individuais que, em conjunto, formam uma ordem espontânea (Hayek, 1978). O resultado deste processo é um "dinheiro honesto", cuja oferta não pode ser facilmente manipulada. A história monetária, no entanto, pode ser vista como o processo pelo qual este dinheiro de mercado é sistematicamente corrompido pelo poder estatal. Através de leis de curso forçado (*legal tender*) e da sanção de práticas bancárias que criam dinheiro sem lastro, o Estado substitui a escolha do mercado por um monopólio coercivo, minando as próprias funções que a moeda deveria servir (Hülsmann, 2008).

2.1.3 O sistema monetário e de pagamentos no Brasil

O sistema monetário brasileiro contemporâneo é o resultado de uma longa e complexa evolução, marcada por um histórico de instabilidade e hiperinflação que levou a sucessivas trocas de moeda ao longo do século XX (Réis, Cruzeiro, Cruzado, entre outros). Essa experiência moldou profundamente a relação da população com o dinheiro e a busca por estabilidade, culminando na implementação do Plano Real em 1994, que finalmente conseguiu controlar a inflação e estabelecer uma base sólida para a economia. A moeda vigente, o Real (BRL), é uma moeda fiduciária, emitida e controlada pelo Banco Central do Brasil (BCB), autarquia federal criada em 1964 com a missão de assegurar a estabilidade do poder de compra da moeda e zelar por um sistema financeiro sólido, eficiente e competitivo (Brasil, 1964).

Paralelamente à estabilização da moeda, o Banco Central promoveu uma profunda modernização na infraestrutura de transações do país, conhecida como Sistema de Pagamentos Brasileiro (SPB). Uma reforma crucial, implementada em 2002, reestruturou o SPB com a criação do Sistema de Transferência de Reservas (STR), um sistema de liquidação bruta em tempo real (LBTR). Conforme informações do próprio Banco Central, o STR funciona como a espinha dorsal do sistema financeiro, processando a liquidação final e irrevogável de transferências interbancárias, garantindo segurança e agilidade para transações de alto valor. Essa modernização reduziu drasticamente o risco sistêmico que existia em modelos de liquidação defasada (Banco Central do Brasil, 2014).

A evolução do SPB não parou. O sistema continuou a incorporar novas tecnologias, como a Transferência Eletrônica Disponível (TED), que ampliou o acesso a transferências rápidas. No entanto, a inovação mais disruptiva e de maior impacto social foi o lançamento do PIX em novembro de 2020. O PIX é um sistema de pagamento instantâneo, operado pelo Banco Central, que permite a transferência de fundos 24 horas por dia, 7 dias por semana, de forma praticamente imediata e com custo baixíssimo ou nulo para o usuário final (Banco central do Brasil, 2020).

Relatórios e estatísticas do Banco Central demonstram que a adoção do PIX foi massiva e exponencial, superando em pouco tempo o número de transações de outros meios de pagamento tradicionais, como DOC, TED e até mesmo cartões de débito e crédito (Banco Central do Brasil, 2023). A simplicidade de uso, através de chaves de endereçamento (CPF, e-

mail, celular ou chave aleatória), e a ampla interoperabilidade entre as instituições financeiras foram fatores-chave para sua popularização. O PIX não apenas otimizou a experiência de pagamento para milhões de brasileiros, mas também promoveu a inclusão financeira e aumentou a competição no setor, forçando uma redução nas taxas de serviços bancários (Banco Central do Brasil, 2023).

Portanto, o cenário brasileiro atual é caracterizado por uma moeda fiduciária estável (o Real) e um sistema de pagamentos centralizado, estatal e extremamente eficiente (o PIX) (Banco Central do Brasil, 2023). Essa combinação representa uma barreira competitiva formidável para a adoção de criptomoedas, como o *Bitcoin*, como meio de pagamento para transações cotidianas. Enquanto o *Bitcoin* oferece uma proposta de valor baseada na descentralização e resistência à censura (Nakamoto, 2008; Ulrich,2014), o PIX entrega uma solução de conveniência, velocidade e baixo custo que atende, de forma eficaz, às necessidades da vasta maioria da população e do comércio no Brasil (Banco central do Brasil, 2020).

2.2 AS PERSPECTIVAS DA ESCOLA AUSTRÍACA SOBRE A NATUREZA DA MOEDA

A arquitetura tecnológica do *Bitcoin* materializa conceitos econômicos que há muito criticavam a estrutura do sistema financeiro tradicional. As teorias da Escola Austríaca de Economia, em particular, oferecem um arcabouço conceitual para analisar o *Bitcoin* como um candidato a "dinheiro sólido" (*sound money*), ou seja, uma moeda que, por suas propriedades intrínsecas, é resistente à manipulação e à degradação do seu valor.

2.2.1 A origem evolutiva e a natureza da moeda

A teoria austríaca sustenta que a moeda não é uma invenção do Estado, mas uma instituição social que emerge espontaneamente das interações de mercado para resolver as ineficiências da troca direta (Menger, 1892). Os indivíduos, buscando facilitar as suas trocas, convergem para o uso de uma mercadoria que possua a maior "vendabilidade" (*salability*). A vendabilidade de um bem é determinada por um conjunto de propriedades: durabilidade, portabilidade, divisibilidade, fungibilidade e, crucialmente, escassez.

Menger (1892, p. 248) define este conceito:

> A vendabilidade (*salability*) de uma mercadoria é [...] a maior ou menor facilidade com que ela pode ser vendida em um mercado a qualquer momento aos preços correntes de compra [...]. Diferentes mercadorias têm diferentes graus de vendabilidade. [...] O interesse econômico dos homens os leva a trocar bens que têm para eles uma utilidade menor por outros que têm uma utilidade maior. Mas seu interesse econômico também os leva a cuidar para que obtenham, na troca, mercadorias cuja vendabilidade seja maior que a dos bens que alienam.

O *Bitcoin* exibe essas propriedades de forma digital. É puramente informacional, portanto, perfeitamente durável e portátil. É divisível até oito casas decimais. Suas unidades são fungíveis na rede. E a sua escassez é absoluta e matematicamente garantida por um algoritmo que limita a sua emissão total a 21 milhões de unidades. O "Teorema da Regressão" de Mises (1953) postula que o valor da moeda hoje deriva da sua utilidade como mercadoria ontem, numa cadeia que remonta ao seu uso não monetário. No caso do *Bitcoin*, o seu valor inicial derivou da sua utilidade para uma comunidade de criptógrafos e entusiastas da tecnologia, que o valorizavam pela sua inovação e potencial como um sistema de pagamento resistente à censura, estabelecendo assim uma base para a sua posterior monetização (Ulrich, 2014). Desta forma, o *Bitcoin* pode ser classificado como um "dinheiro-mercadoria" digital, cujo valor reside nas suas propriedades intrínsecas e na robustez da sua rede, e não num decreto governamental (Rothbard, 2009).

2.2.2 A crítica ao sistema fiduciário e a defesa de uma política monetária previsível

O sistema monetário contemporâneo, baseado em moedas fiduciárias, é criticado por conceder aos governos o monopólio da emissão monetária, um poder que, historicamente, leva à desvalorização da moeda via inflação para financiar gastos estatais (Mises, 2010; Rothbard, 2008). Adicionalmente, o sistema bancário de reservas fracionárias permite a expansão de crédito desvinculado da poupança real.

Huerta de Soto (2012, p. 35) define a natureza deste mecanismo:

> Com efeito, o sistema bancário de reserva fracionária consiste em criar "recibos de depósito" (em forma de notas ou depósitos à vista) que não correspondem a depósitos prévios de dinheiro [...]. O sistema bancário, portanto, cria "dinheiro" do nada (na medida em que os recibos de depósito à vista cumprem todas as funções do dinheiro) e o injeta na economia através do crédito concedido aos seus clientes. Este processo de expansão creditícia é a causa única por trás dos ciclos econômicos [...].

A constante manipulação da oferta monetária impede que o dinheiro cumpra a sua função mais importante numa economia complexa: a de ser uma ferramenta estável para o cálculo econômico, impossibilitando que empresários avaliem corretamente os seus investimentos e aloquem capital de forma eficiente a longo prazo (Mises, 2010). A política monetária do *Bitcoin* foi desenhada como uma antítese a este modelo. Com uma oferta final limitada e uma taxa de emissão predeterminada e decrescente, o seu protocolo elimina a possibilidade de manipulação discricionária. Esta previsibilidade e rigidez são a manifestação prática do ideal de dinheiro sólido, imune às pressões políticas que historicamente degradaram o poder de compra das moedas estatais. Para seus proponentes, esta é a sua característica mais importante, pois oferece uma âncora de estabilidade num mundo de políticas monetárias expansionistas (Ulrich, 2014).

2.2.3 A concretização da desestatização do dinheiro

Hayek (2011) propôs que a única forma de obter um dinheiro de qualidade seria abolir o monopólio governamental e permitir que emissores privados competissem livremente. O autor argumenta que o mercado é o único mecanismo capaz de selecionar um dinheiro estável (Hayek, 2011, p. 78):

> Não há razão para duvidar que a concorrência do mercado privado seja, em geral, mais eficiente na descoberta dos melhores métodos de satisfação das necessidades humanas do que o são os organismos governamentais. [...] Não há exemplo, que eu saiba, de um governo que tenha fornecido voluntariamente ao seu povo, durante um período considerável, um dinheiro bom, a não ser quando obrigado a fazê-lo, como, por exemplo, pela necessidade de competir com outro dinheiro.

O *Bitcoin* representa a primeira implementação bem-sucedida desta ideia, não por uma reforma política, mas por uma disrupção tecnológica que criou um sistema monetário paralelo e global, fora do controle de qualquer Estado. A sua existência força uma comparação direta com as moedas fiduciárias, tornando as suas falhas, como a inflação, mais evidentes para o público e funcionando como um contraponto disciplinar. Assim, o *Bitcoin* encarna a ideia de que a separação entre o dinheiro e o Estado é fundamental para a liberdade econômica (Rothbard, 2009).

2.3 A MOEDA NA PERSPECTIVA LIBERAL

A tradição do pensamento liberal, desde seus primórdios, expressa uma profunda desconfiança em relação à concentração de poder no Estado, especialmente no que tange ao controle sobre a moeda. A preocupação central é que a autoridade monetária, quando exercida de forma discricionária, invariavelmente se torna uma ferramenta de poder arbitrário, prejudicando a liberdade econômica e a estabilidade social (Friedman, 2014; Smith, 1996). Tanto a vertente clássica de Adam Smith quanto a monetarista de Milton Friedman compartilham a visão de que a intervenção governamental na esfera monetária é uma fonte primária de instabilidade.

Smith (1996) via a moeda como uma tecnologia social que emerge espontaneamente do mercado para facilitar as trocas, sendo o papel legítimo do governo o de certificar a qualidade da moeda, como um selo que atesta o peso e a pureza do metal. Contudo, ele alertava que a "avareza e a injustiça dos príncipes e dos Estados soberanos", ao longo da história, os levaram a diminuir a quantidade de metal puro que as moedas continham, um expediente fraudulento para liquidar dívidas e financiar despesas, efetivamente enganando os credores e a população. Essa degradação monetária, segundo Smith, é uma das maiores ameaças à propriedade privada e à previsibilidade necessária para o florescimento do comércio (Smith, 1996).

Essa crítica é aprofundada por Friedman (2014), que argumenta que a inflação é, sempre e em toda parte, um fenômeno monetário, resultante de um aumento na quantidade de moeda mais rápido do que o aumento da produção. Friedman via a capacidade do governo de imprimir dinheiro como uma forma de impor um "imposto inflacionário", uma tributação sem representação que corrói silenciosamente o poder de compra e a poupança dos cidadãos.

O autor demonstra a relação entre o poder governamental e a degradação da moeda (Friedman, 2014, p. 115-116):

> A inflação é, em si, um imposto. É um imposto sobre os saldos monetários. [...] Quando o governo imprime dinheiro (ou o Banco Central cria depósitos) para financiar seus gastos, ele obtém recursos reais em troca. Os detentores de dinheiro pagam o imposto porque o valor real de seus saldos monetários é depreciado pela subsequente elevação dos preços. [...] Esta é uma forma de tributação sem representação, pois nem a taxa nem a receita são explicitamente autorizadas por aqueles que são forçados a pagá-la.

A solução de Friedman não era necessariamente retornar a uma moeda-mercadoria, mas sim substituir a discricionariedade das autoridades por regras claras e previsíveis, como uma taxa de crescimento monetário constante e publicamente conhecida. O objetivo central era tornar a política monetária automática e transparente, removendo o poder arbitrário das mãos de burocratas e submetendo o governo a um princípio de legalidade monetária (Friedman, 2014). Assim, a perspectiva liberal converge na defesa de uma moeda previsível e protegida da manipulação política. O *Bitcoin*, com sua política monetária algorítmica, transparente e imutável, pode ser interpretado como uma resposta tecnológica a essa demanda liberal por "regras, não governamentais", materializando em código a busca por um dinheiro honesto e confiável.

2.4 A INOVAÇÃO TECNOLÓGICA DO *BLOCKCHAIN*

A proposta de Nakamoto (2008) em "*Bitcoin*: um Sistema de Dinheiro Eletrônico *Peer-to-Peer*" foi criar um sistema que permitisse pagamentos online diretos sem a intermediação de uma instituição financeira. O principal desafio tecnológico para tal sistema

era o "problema do gasto duplo", um risco inerente a qualquer ativo digital que, por sua natureza informacional, pode ser facilmente copiado. A solução do *Bitcoin* é uma arquitetura descentralizada que combina uma rede *peer-to-peer* (P2P), um mecanismo de consenso por Prova-de-Trabalho (*Proof-of-Work*) e um livro-razão público e imutável, o *blockchain*.

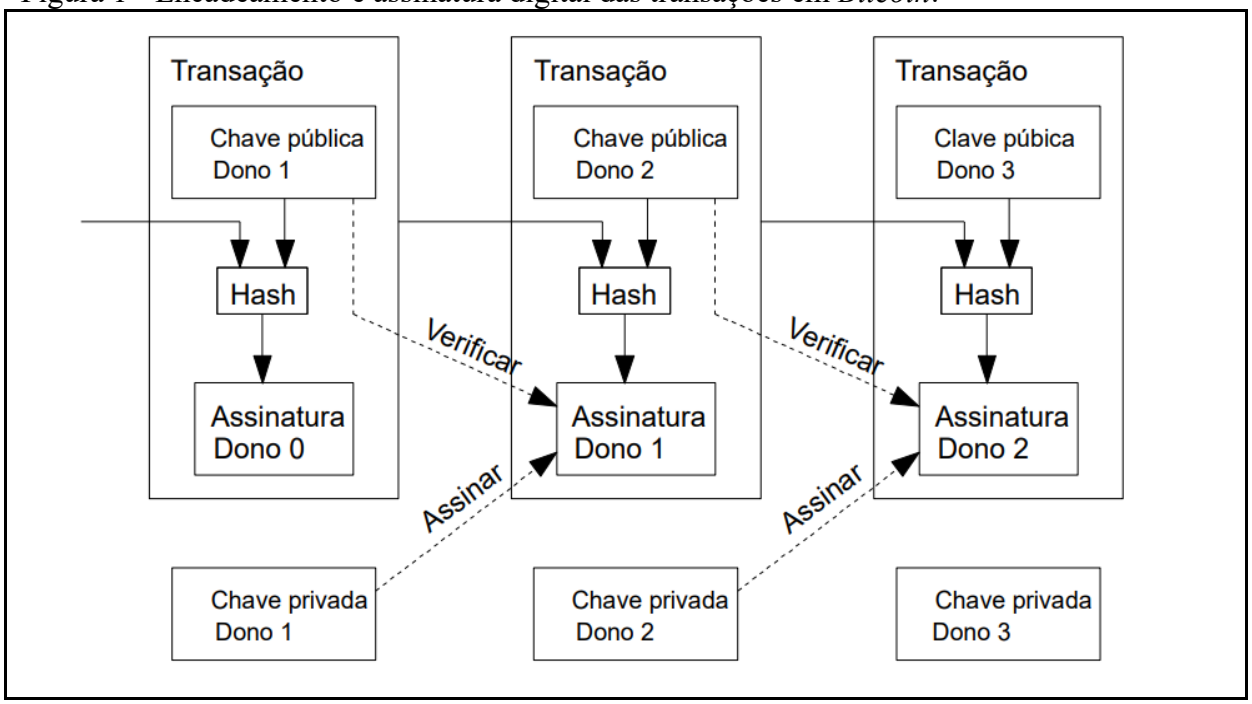
Nakamoto (2008, p. 1) define sua própria proposta:

> Uma versão puramente *peer-to-peer* de dinheiro eletrônico permitiria que pagamentos online fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira. Assinaturas digitais fornecem parte da solução, mas os principais benefícios são perdidos se um terceiro confiável ainda for necessário para evitar o gasto duplo. Propomos uma solução para o problema do gasto duplo usando uma rede *peer-to-peer*. A rede carimba as transações com data e hora, colocando-as em uma cadeia contínua de prova-de-trabalho baseada em *hash*, formando um registro que não pode ser alterado sem refazer a prova-de-trabalho.

Juntos, esses componentes criam um sistema de "confiança por computação", no qual a integridade é garantida por matemática e teoria dos jogos, em vez de por uma autoridade central (Antonopoulos, 2017).

Nesta rede, as transações são validadas e adicionadas em blocos cronológicos, formando uma cadeia contínua. A imutabilidade do registo é assegurada pelo encadeamento criptográfico: cada bloco contém um *hash* (uma assinatura digital única) do bloco anterior, criando uma dependência que torna o histórico computacionalmente impraticável de ser alterado (Narayanan *et al*., 2016). A Figura 1, extraída do artigo original de Nakamoto (2008), ilustra esse processo de encadeamento.

Figura 1 - Encadeamento e assinatura digital das transações em *Bitcoin*.



Fonte: Nakamoto (2008, p. 2).

A tecnologia *blockchain* é, em essência, uma base de dados distribuída que registra transações de forma segura e transparente. A sua natureza pública e permissão, no caso do *Bitcoin*, significa que qualquer pessoa pode auditar o livro-razão e participar na validação das transações, o que promove um elevado grau de transparência e resistência à censura (Yano *et al*., 2020).

O processo de adicionar novos blocos, conhecido como mineração, exige um grande esforço computacional. É este custo real, em energia e poder de processamento, que ancora a segurança da rede ao mundo físico, garantindo a sua integridade sem a necessidade de uma autoridade central para validar as operações (Nakamoto, 2008; Courtois; Grajek; Naik, 2014). Os mineradores são incentivados economicamente a agir de forma honesta através da recompensa de bloco (novos *bitcoins*) e das taxas de transação, um modelo que alinha os interesses individuais com a segurança coletiva da rede. Este mecanismo de incentivos é crucial para a sustentabilidade e robustez do sistema a longo prazo (Yano *et al*., 2020).

Por fim, a segurança da propriedade é assegurada por criptografia de chave pública, onde cada utilizador possui um par de chaves (pública e privada). A posse da chave privada confere ao seu detentor o controle soberano sobre os seus fundos, permitindo-lhe realizar transações de forma autónoma e segura, como se fosse um ativo ao portador digital (Ulrich, 2014). A combinação destes elementos um livro-razão distribuído, um consenso baseado em custos e incentivos, e a soberania do utilizador constitui a inovação fundamental que permite ao *Bitcoin* funcionar como um sistema de pagamento global sem depender de intermediários tradicionais.

2.4.1 A camada de pagamentos: *Lightning Network* e escalabilidade

Embora o protocolo base do *Bitcoin* ofereça segurança e descentralização sem precedentes, sua arquitetura impõe limites físicos à quantidade de transações processadas por segundo, o que gera gargalos e taxas elevadas em momentos de alta demanda na rede (Antonopoulos; Osuntokun; Pickhardt, 2022). Atualmente, a rede principal suporta cerca de sete transações por segundo, e qualquer tentativa de aumentar essa capacidade via expansão do tamanho dos blocos para níveis globais poderia levar ao colapso do sistema ou à centralização extrema dos nós, uma vez que as exigências de armazenamento e largura de banda excederiam as capacidades de computadores domésticos (Khan; State, 2019). Para viabilizar o uso do *Bitcoin* em transações cotidianas de baixo valor, surge a *Lightning Network* (LN), uma solução de segunda camada que opera sobre o *blockchain* principal, permitindo pagamentos instantâneos e de custo virtualmente nulo (Antonopoulos; Osuntokun; Pickhardt, 2022).

A LN funciona através da abertura de canais bidirecionais entre usuários, onde as transações ocorrem de forma privada e fora da rede principal, ou *off-chain* (Antonopoulos; Osuntokun; Pickhardt, 2022). Nesse modelo, as partes podem realizar um número infinito de transferências fora da rede, com o custo total equivalente ao registro de apenas duas transações no *blockchain* do *Bitcoin* (Khan; State, 2019). Conforme explicam Antonopoulos, Osuntokun e Pickhardt (2022), apenas a abertura e o fechamento do canal são registrados no *blockchain*, o que reduz drasticamente a carga de dados processada pelos mineradores na camada base.

Diferente da camada base, onde a confirmação de um bloco leva em média dez minutos, as transações na LN são liquidadas na velocidade da comunicação entre computadores (Antonopoulos; Osuntokun; Pickhardt, 2022). Essa característica permite a execução de micropagamentos, um setor de mercado com grande potencial inexplorado devido aos custos operacionais dos métodos tradicionais (Antonopoulos; Osuntokun; Pickhardt, 2022). Assim, o *Bitcoin* torna-se tecnicamente competitivo frente a soluções instantâneas centralizadas, como o PIX no cenário nacional, além de possibilitar fluxos de transações transfronteiriças mais ágeis e baratos que os métodos convencionais (Khan; State, 2019; Antonopoulos; Osuntokun; Pickhardt, 2022).

A rede permite que pagamentos sejam enviados através de uma teia de canais interconectados, utilizando a teoria dos grafos para encontrar o caminho mais eficiente entre o pagador e o recebedor sem a necessidade de um canal direto entre ambos (Antonopoulos; Osuntokun; Pickhardt, 2022). Para assegurar a integridade e o anonimato nesse processo, o

protocolo utiliza o roteamento em cebola (*onion routing*), garantindo que intermediários não identifiquem a origem ou o destino final dos fundos (Khan; State, 2019). Esse sistema de roteamento é fundamental para garantir a escalabilidade do ecossistema sem comprometer a custódia própria dos ativos (Antonopoulos; Osuntokun; Pickhardt, 2022).

A integridade das operações na LN é mantida por contratos inteligentes que empregam tecnologias de múltiplas assinaturas (*multisignature*) e travas de tempo (*locktime*), dispensando a necessidade de confiança mútua entre as partes ou intermediários (Khan; State, 2019). Caso uma das partes tente agir de forma desonesta, os mecanismos de penalidade do protocolo permitem que a parte prejudicada recupere os fundos, mantendo o incentivo econômico para a cooperação (Antonopoulos; Osuntokun; Pickhardt, 2022). Embora ofereça vantagens de velocidade e custo, é importante ressaltar que a LN fornece transações teoricamente menos seguras que a rede principal, o que orienta sua aplicação preferencial para valores menores (Khan; State, 2019).

Sob a ótica administrativa, a *Lightning Network* transforma o *Bitcoin* de um ativo estático de reserva de valor em um sistema dinâmico de transferência de riqueza (Antonopoulos; Osuntokun; Pickhardt, 2022). Essa evolução tecnológica mitiga o problema das taxas de rede que, historicamente, inviabilizavam sua função monetária primária nas transações de varejo (Antonopoulos; Osuntokun; Pickhardt, 2022).

2.5 TEORIA DOS JOGOS E A SEGURANÇA DA REDE *BITCOIN*

A robustez do *Bitcoin* não deriva da benevolência de seus participantes, mas de um engenhoso sistema de incentivos econômicos que pode ser rigorosamente analisado pela ótica da Teoria dos Jogos. O design de Nakamoto (2008) intencionalmente criou um "jogo" no qual a estratégia mais racional e lucrativa para cada participante (minerador), assumindo que buscam maximizar seus lucros, é agir honestamente e seguir as regras do protocolo. A segurança da rede emerge, portanto, como um equilíbrio de Nash: uma situação estável onde nenhum agente tem incentivo para se desviar unilateralmente do comportamento honesto, dado que todos os outros também estão agindo honestamente (Warren, 2023).

Cada minerador enfrenta uma escolha estratégica: seguir as regras do protocolo para tentar adicionar o próximo bloco válido e receber a recompensa, ou tentar fraudar o sistema, por exemplo, através de um "ataque de 51%". Este tipo de ataque exigiria que um agente malicioso controlasse a maior parte do poder computacional da rede para criar uma cadeia de blocos alternativa e reverter suas próprias transações (gasto duplo) (Nakamoto, 2008). No entanto, a matriz de pagamentos torna essa estratégia economicamente irracional (Warren, 2023).

Primeiro, o custo para adquirir e operar mais de 50% do poder de *hash* da rede global é proibitivo, exigindo um investimento massivo em hardware e energia (Kroll; Davey; Felten, 2013). Segundo, mesmo que um ataque fosse bem-sucedido, ele apenas permitiria ao atacante reverter suas próprias transações; não lhe daria o poder de roubar *Bitcoins* de outros usuários ou alterar as regras fundamentais do protocolo. Terceiro, e mais importante, um ataque bem-sucedido e publicamente conhecido destruiria a confiança na segurança e imutabilidade do *Bitcoin*, fazendo seu preço de mercado colapsar. Isso aniquilaria o valor do próprio ativo que o atacante estaria tentando manipular, além de tornar seu massivo investimento em hardware de mineração obsoleto (Budish, 2018).

Portanto, a Teoria dos Jogos revela que a estratégia dominante para um minerador racional é a cooperação. O benefício de seguir as regras (receber recompensas de bloco e taxas) é direto, previsível e alinhado com a valorização do ativo a longo prazo. O ataque tem um custo proibitivo, um ganho potencial limitado e um risco existencial para o próprio investimento (Warren, 2023). O *Bitcoin* transforma o autointeresse e a competição, tradicionalmente vistos

como forças potencialmente caóticas, nos pilares de sua própria segurança, criando uma ordem descentralizada e confiável sem a necessidade de um supervisor central. A robustez do sistema não depende da bondade dos participantes, mas da sua racionalidade econômica dentro da estrutura de incentivos cuidadosamente desenhada pelo protocolo (Nakamoto, 2008; Warren, 2023).

2.6 O CENÁRIO REGULATÓRIO BRASILEIRO

A ascensão de uma tecnologia monetária descentralizada representa um desafio fundamental à soberania do Estado, cuja autoridade se assenta no controle sobre a moeda e os fluxos financeiros. A trajetória da regulação brasileira pode ser entendida não como uma tentativa de proibir a inovação, mas como uma manobra estratégica para conter o seu potencial disruptivo, canalizando-a para um ecossistema supervisionado. A estratégia foi focar nos intermediários os pontos de acesso ao sistema em vez do protocolo em si, que opera fora de qualquer jurisdição nacional.

2.6.1 A definição do ativo e a exclusão monetária (BACEN e CVM)

A primeira reação do Estado brasileiro foi definir a natureza jurídica do *Bitcoin*. O Comunicado nº 25.306 do Banco Central (Brasil, 2014) foi um movimento crucial. Ao classificar o *Bitcoin* como um "ativo virtual" e não como "moeda eletrônica", o Bacen negou-lhe o estatuto de moeda. Essa distinção foi fundamental, pois removeu o *Bitcoin* da esfera da política monetária e da legislação de curso forçado, tratando-o legalmente como uma mercadoria ou um bem intangível. Isso, por um lado, permitiu que o mercado se desenvolvesse sem incorrer em ilegalidade, mas, por outro, abriu o caminho para a sua tributação como um ativo gerador de ganho de capital. A Comissão de Valores Mobiliários (CVM), através do Parecer de Orientação nº 40 (Brasil, 2022b), complementou esta abordagem ao concluir que o *Bitcoin*, pela sua natureza descentralizada, não se enquadra como valor mobiliário, focando a sua atenção em ativos digitais que se assemelham a ofertas de investimento.

2.6.2 A ferramenta de controlo: vigilância fiscal (Receita Federal do Brasil)

Uma vez definido como ativo tributável, o passo seguinte foi criar um mecanismo de vigilância. A Instrução Normativa RFB nº 1.888 (Brasil, 2019) transformou as corretoras (*exchanges*) em agentes de fiscalização, exigindo o reporte mensal de todas as operações. Esta medida, aliada à tributação sobre ganhos de capital (IRPF), impõe um atrito significativo ao uso do *Bitcoin* como meio de pagamento. Cada vez que um cidadão utiliza *Bitcoin* para comprar um bem ou serviço, ele está, para fins fiscais, realizando uma alienação de um ativo. Se o valor em Reais do *Bitcoin* no momento da compra for superior ao seu valor de aquisição, o ganho de capital deve ser apurado e, se o total de alienações no mês exceder o limite de isenção, o imposto é devido. Isso transforma cada pequena transação quotidiana num evento contabilístico complexo, desincentivando ativamente a sua função de meio de troca e incentivando o uso da moeda fiduciária oficial.

2.6.3 A consolidação da estratégia: o marco legal dos Criptoativos (Lei nº 14.478/2022)

A aprovação do Marco Legal dos Criptoativos (Brasil, 2022a) estabeleceu as diretrizes fundamentais, focando-se nos "prestadores de serviços de ativos virtuais" (VASPs) e submetendo-os à supervisão do Banco Central. A lei impôs requisitos de governança, gestão de riscos e políticas de Prevenção à Lavagem de Dinheiro (PLD/FT), conferindo legitimidade ao

setor enquanto "domesticava" a tecnologia para o ambiente institucional. Contudo, a efetiva operacionalização desse mercado dependia da regulamentação infralegal do BCB, que detalhou as exigências de capital e funcionamento.

2.6.4 O marco regulatório infralegal: resoluções BCB nº 519, 520 e 521

Em 10 de novembro de 2025, o Banco Central do Brasil publicou um pacote normativo decisivo, as Resoluções BCB nº 519, 520 e 521, que entrou em vigor em 2 de fevereiro de 2026, estabelecendo o padrão operacional "nível banco" para o setor. Esta regulamentação criou a figura jurídica das Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs), classificadas em três modalidades principais: intermediárias, custodiantes e corretoras de ativos virtuais (Banco Central do Brasil, 2025).

A Resolução BCB nº 520 instituiu a obrigatoriedade da segregação patrimonial, exigindo que os recursos dos clientes sejam mantidos em contas separadas do patrimônio da corretora, mitigando riscos de insolvência e uso indevido de fundos. Adicionalmente, as SPSAVs passaram a responder integralmente por perdas causadas por negligência e a seguir padrões rigorosos de segurança cibernética (Banco Central do Brasil, 2025).

A Resolução BCB nº 521 regulamentou o uso de ativos virtuais em operações de câmbio e transferências internacionais, submetendo o envio de valores para o exterior a regras de monitoramento similares às remessas tradicionais (Banco Central do Brasil, 2025). Tal medida reforça a estratégia estatal de integrar os fluxos descentralizados ao controle das autoridades financeiras (Brasil, 2022a).

Para alinhar o país às práticas internacionais de combate a ilícitos (*Travel Rule*), a IN nº 704 organizou o processo de autorização em fases. A partir de 4 de maio de 2026, torna-se obrigatória a prestação mensal de informações detalhadas ao Banco Central sobre todas as transações, incluindo a identificação de titulares de carteiras de origem e destino (Banco Central do Brasil, 202).

Para as empresas que já operavam no país, foi estabelecido um prazo até 30 de outubro de 2026 para o protocolo do pedido de autorização definitiva junto ao BCB, sob pena de encerramento das atividades ((Banco Central do Brasil, 2025). Este cronograma visa garantir a transição ordenada para o novo regime de supervisão direta da autarquia (Brasil, 2022a).

Essa estrutura regulatória remove a "zona cinzenta" em que operavam as *exchanges* e impõe um custo de conformidade elevado, o que, sob a ótica da Administração, pode levar a uma consolidação do mercado no Brasil, privilegiando grandes *players* em detrimento de novos entrantes menos capitalizados (BRASIL, 2022a).

3 PROCEDIMENTOS METODOLÓGICOS

O método científico é um conjunto de procedimentos sistemáticos usado de forma racional para investigar fenômenos, a fim de fornecer novos conhecimentos ou integrar informações a conhecimentos já existentes. Segundo Gil (2022), trata-se de um procedimento racional e sistemático que tem como objetivo fornecer respostas aos problemas que são propostos.

Neste capítulo são apresentados os métodos utilizados para a coleta e análise das informações, conceituando os pilares que embasam este trabalho. O objetivo deste estudo buscou responder à pergunta: "Qual a viabilidade, sob as óticas de execução, base teórica e regulatória, do *Bitcoin* como meio de pagamento no Brasil?".

Quanto aos fins de investigação, a pesquisa caracteriza-se como exploratória. Segundo Gil (2008), as pesquisas exploratórias têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a

construir hipóteses. Esta abordagem é adequada, pois a viabilidade do *Bitcoin* como meio de pagamento no Brasil é um fenômeno tecnológico e econômico emergente, e o planejamento da pesquisa tende a ser flexível para considerar os variados aspectos do fenômeno.

Quanto aos meios, a pesquisa se definiu como bibliográfica e documental. Vergara (1998) descreve a pesquisa bibliográfica como um estudo sistematizado fundamentado em material acessível ao público em geral, como livros, periódicos e redes eletrônicas.

A autora ressalta ainda que esse método fornece instrumental analítico essencial para qualquer tipo de pesquisa, podendo também esgotar-se em si mesmo. Conforme Marconi e Lakatos (2003), a pesquisa bibliográfica é o "primeiro passo em qualquer tipo de pesquisa científica", permitindo ao pesquisador revisar a literatura existente sobre o tema.

O estudo utilizou exclusivamente dados secundários. Segundo Gil (2022), dados secundários são aqueles que já foram coletados, tabulados, ordenados e, às vezes, até analisados, estando à disposição dos interessados. Neste TCC, os dados secundários são compostos por todo o material bibliográfico livros, artigos científicos, relatórios e estatísticas do Banco Central bem como pelos textos de legislação, como a Lei nº 14.478/2022 e a Instrução Normativa RFB nº 1.888/2019, que foram analisados para responder ao problema de pesquisa.

A análise dos dados foi realizada sob abordagem qualitativa, que opera de forma indutiva, focando na construção de padrões e temas a partir dos dados (Creswell, 2010). O método empregado foi a análise bibliográfica, por meio da qual os conteúdos das fontes levantadas obras seminais da Escola Austríaca, artigos técnicos sobre protocolos de pagamento e documentos normativos foram sistematicamente identificados, selecionados e confrontados entre si, permitindo identificar convergências, divergências e lacunas interpretativas entre os diferentes autores e instrumentos normativos. Diferentemente da análise de conteúdo, que foca na categorização temática de mensagens, a análise bibliográfica permitiu construir um quadro interpretativo integrado, no qual os resultados são discutidos em diálogo direto com a literatura especializada e com o arcabouço legislativo mapeado (Vergara, 1998; Marconi; Lakatos, 2003).

Para a seleção das fontes, foram adotados critérios de inclusão e exclusão. Constituíram critérios de inclusão: (a) obras de referência reconhecida nas áreas de teoria monetária austríaca, economia liberal e tecnologia de criptoativos; (b) artigos técnicos sobre protocolos de *blockchain* e *Lightning Network* publicados em periódicos ou repositórios revisados por pares; (c) documentos normativos emitidos por órgãos regulatórios brasileiros Banco Central, Receita Federal e CVM vigentes até o primeiro semestre de 2026. Foram excluídas obras sem identificação de autoria verificável, textos de opinião sem embasamento acadêmico e fontes não indexadas em bases de dados científicas. O período de análise do material bibliográfico compreende publicações de 1892 a 2026, com ênfase nas obras regulatórias e técnicas produzidas a partir de 2014, ano do primeiro posicionamento oficial do Banco Central do Brasil sobre criptoativos. A coleta e análise do material ocorreram entre os meses de agosto de 2025 e maio de 2026.

O processo de análise seguiu as seguintes etapas: (1) Organização e preparação: os documentos bibliográficos e documentais foram organizados por eixo temático teoria monetária, arquitetura técnica, análise comparativa e cenário regulatório. (2) Leitura e exploração: foi realizada leitura sistemática de todo o material para identificar os argumentos centrais de cada autor e norma. (3) Confronto e síntese: os argumentos foram confrontados entre si, identificando onde os autores convergem, divergem ou se complementam. (4) Interpretação: os resultados e temas foram interpretados, confrontando a teoria com a prática e a regulação para responder à pergunta de pesquisa, conforme apresentado na seção seguinte.

4 PESQUISA E DISCUSSÃO DE RESULTADOS

Esta seção apresenta os resultados da pesquisa bibliográfica e documental realizada, organizando os achados em quatro eixos analíticos interligados: (4.1) a avaliação do *Bitcoin* como candidato a meio de troca com base na teoria monetária austríaca; (4.2) o ecossistema técnico de pagamentos em *Bitcoin* e a *Lightning Network*; (4.3) o estudo comparativo entre o *Bitcoin/Lightning Network* e os principais sistemas de pagamento em uso no Brasil; e (4.4) o cenário regulatório brasileiro como condicionante da viabilidade. A organização sequencial dessas dimensões permite construir uma resposta integrada ao problema de pesquisa, confrontando a promessa teórica do *Bitcoin* com a realidade prática e regulatória do contexto nacional.

4.1 O *BITCOIN* COMO CANDIDATO A MEIO DE TROCA: UMA ANÁLISE MONETÁRIA

O ponto de partida para avaliar a viabilidade do *Bitcoin* como meio de pagamento é verificar se ele satisfaz os critérios que definem uma moeda de qualidade segundo a tradição teórica que fundamenta este trabalho. Conforme estabelecido por Menger (1892), o mercado converge para aquela mercadoria que apresenta maior "vendabilidade" conceito que sintetiza um conjunto de propriedades físicas e econômicas que tornam um bem apto a ser universalmente aceito em trocas. As propriedades centrais identificadas pela Escola Austríaca são: escassez, durabilidade, portabilidade, divisibilidade, fungibilidade e resistência à manipulação estatal.

A fim de sistematizar essa avaliação, o Quadro 1 apresenta uma análise comparativa entre o *Bitcoin* e o padrão histórico de "dinheiro sólido" (*sound money*) por excelência — o ouro — segundo cada um dos critérios monetários identificados na fundamentação teórica.

Quadro 1 – Análise comparativa do *Bitcoin* em relação aos critérios monetários da escola austríaca

CRITÉRIO MONETÁRIO (ESCOLA AUSTRÍACA)	MOEDA-MERCADORIA (OURO)	*BITCOIN*
Escassez	Limitada; nova oferta via descobertas geológicas e inovação técnica de mineração	Absoluta: 21 milhões de unidades; algoritmo imutável sem consenso da rede
Durabilidade	Alta, porém sujeita à corrosão física e desgaste em circulação	Perfeita: informação digital não se deteriora com o tempo
Portabilidade	Limitada pelo peso e volume; custódia e transporte custosos	Ilimitada: transferível globalmente em segundos via internet, sem fronteiras
Divisibilidade	Divisível, porém com custo de fundição e cunhagem	Até 8 casas decimais (1 satoshi = 0,00000001 BTC), sem custo adicional
Fungibilidade	Alta entre metais de mesma pureza e cunhagem reconhecida	Alta na rede; rastreabilidade do *blockchain* gera debate sobre fungibilidade perfeita
Resistência à manipulação estatal	Baixa: o Estado substituiu o padrão-ouro por moedas fiduciárias ao longo do séc. XX	Alta: protocolo descentralizado impede qualquer autoridade de alterar a política monetária
Origem do valor (Teorema da Regressão)	Uso não-monetário como ornamento e insumo industrial precede o monetário.	Utilidade inicial como ferramenta criptográfica para comunidade técnica específica

Fonte: Elaborado pelo autor com base em Menger (1892), Mises (1953), Rothbard (2013) e Ulrich (2014).

A análise do Quadro 1 revela que o *Bitcoin* não apenas replica as propriedades do ouro, mas as supera em dimensões críticas para a economia digital. A escassez algorítmica com emissão máxima de 21 milhões de unidades, definida no próprio código-fonte e imutável sem o consenso distribuído da rede representa um avanço qualitativo em relação à escassez geológica do ouro, que pode, em princípio, ser ampliada por novas descobertas ou inovações em técnicas de mineração. Mises (1953) argumentava que a moeda de qualidade deveria ter sua oferta determinada por forças de mercado, não por decisões políticas discricionárias. O *Bitcoin* leva esse princípio ao seu limite lógico: a política monetária é determinada por um algoritmo público, verificável e não sujeito a pressões políticas.

A portabilidade perfeita do *Bitcoin* a capacidade de transferir qualquer valor monetário para qualquer lugar do mundo em minutos, sem depender de intermediários resolve a principal limitação histórica do ouro como meio de pagamento nas economias modernas. Como observa Ulrich (2014), o ouro exigiu a intermediação de bancos e, posteriormente, a emissão de notas representativas, processo que abriu caminho para o abandono do lastro e a instauração do sistema fiduciário. O *Bitcoin*, ao ser nativamente digital, elimina essa necessidade estrutural de intermediação.

No que tange ao Teorema da Regressão de Mises (1953), a objeção de que o *Bitcoin* não teria um valor não-monetário original a partir do qual seu valor monetário poderia ter se desenvolvido encontra resposta na análise de Ulrich (2014) o valor inicial do *Bitcoin* derivou de sua utilidade percebida como ferramenta criptográfica e sistema de pagamento resistente à censura para uma comunidade técnica específica. Esse uso original, embora intangível, constituiu o ponto de partida para a cadeia de valor que levou à sua monetização gradual. Sob esse ângulo, o *Bitcoin* se qualifica como um "dinheiro-mercadoria digital" (Rothbard, 2009), cujo valor emerge da sua utilidade técnica e da robustez da rede, e não de um decreto governamental.

A única dimensão em que o *Bitcoin* apresenta ambiguidade é a fungibilidade. Embora as unidades sejam tecnicamente intercambiáveis na rede, a natureza pública e auditável do *blockchain* o rastreamento do histórico de cada unidade. Ferramentas de análise de *blockchain* utilizadas por *exchanges* e autoridades regulatórias podem identificar *bitcoins* associados a atividades ilícitas e recusar-se a aceitá-los, criando uma diferenciação de fato entre unidades formalmente idênticas. Esse ponto representa uma tensão genuína, ainda que protocolos de privacidade, como a *Lightning Network* com seu roteamento em cebola *(onion routing*), mitiguem parcialmente esse problema (Antonopoulos; Osuntokun; Pickhardt, 2022). Em síntese, o *Bitcoin* atende de forma robusta à maioria dos critérios monetários definidos pela Escola Austríaca, consolidando sua qualificação teórica como candidato legítimo à função de meio de troca, ainda que desafios práticos significativos se interponham entre a teoria e a realidade.

4.2 O ECOSSISTEMA TÉCNICO DE PAGAMENTOS: DA REDE BASE À *LIGHTNING NETWORK*

A análise da viabilidade executiva do *Bitcoin* como meio de pagamento exige uma compreensão clara de sua arquitetura em duas camadas e de como cada uma delas se posiciona para diferentes casos de uso no espectro de pagamentos. A rede base (*Layer* 1), cujo protocolo foi descrito por Nakamoto (2008), oferece garantias máximas de segurança e imutabilidade, mas ao custo de uma capacidade de processamento limitada. A *Lightning Network* (*Layer* 2), construída sobre a rede base, propõe resolver o trilema da escalabilidade sem sacrificar os princípios de descentralização e custódia própria dos ativos.

Na rede base, a confirmação de uma transação requer que ela seja incluída em um bloco e que blocos subsequentes sejam adicionados à cadeia, um processo que, em média, leva

dez minutos por bloco. Para pagamentos de alto valor onde a irreversibilidade é crítica como liquidações interbancárias ou aquisições de ativos significativos, aguardar seis confirmações (aproximadamente uma hora) é considerado padrão de segurança aceitável (Narayanan et al., 2016). Esse modelo é funcionalmente incompatível com o varejo físico, onde o consumidor não pode aguardar uma hora para que sua compra seja confirmada.

A *Lightning Network* aborda esse problema estruturalmente. Conforme explicam Antonopoulos, Osuntokun e Pickhardt (2022), o mecanismo central da LN consiste na abertura de canais de pagamento bidirecionais, nos quais as partes depositam uma quantidade de *Bitcoin* em um endereço de múltiplas assinaturas registrado no *blockchain*. A partir desse momento, as transações entre as partes ocorrem de forma privada e instantânea fora da cadeia principal (*off-chain*), representando apenas atualizações do saldo interno do canal. Apenas a abertura e o fechamento do canal são registrados no *blockchain*, comprimindo um número potencialmente ilimitado de micropagamentos em apenas dois registros na rede base.

A inovação da LN vai além dos canais diretos. A rede permite que um pagamento percorra múltiplos canais interconectados para alcançar um destinatário com quem o pagador não possui canal direto, utilizando teoria dos grafos para encontrar o caminho de menor custo e maior liquidez disponível (Antonopoulos; Osuntokun; Pickhardt, 2022). A privacidade nesse roteamento é garantida pelo protocolo de roteamento em cebola (*onion routing*), pelo qual cada nó intermediário conhece apenas o nó anterior e o seguinte no caminho, mas não a origem ou o destino final dos fundos (Khan; State, 2019). Esse mecanismo endereça simultaneamente os problemas de escalabilidade e de privacidade.

A integridade das transações *off-chain* é mantida por contratos inteligentes que empregam travas de tempo (*locktime*) e chaves de revogação. Caso uma das partes tente fechar o canal de forma fraudulenta publicando um estado de saldo desatualizado que lhe seja mais favorável, o protocolo permite que a parte prejudicada recupere todos os fundos do canal como penalidade (Antonopoulos; Osuntokun; Pickhardt, 2022). Esse sistema de penalidades cria o incentivo econômico para que as partes ajam de forma honesta, reproduzindo, na camada de pagamentos, o mesmo alinhamento de incentivos que a Teoria dos Jogos identifica na segurança da rede base (Warren, 2023).

Sob a ótica gerencial, a *Lightning Network* transforma o *Bitcoin* de um instrumento de reserva de valor em um sistema dinâmico de transferência de riqueza capaz de processar micropagamentos com custo virtualmente nulo (Antonopoulos; Osuntokun; Pickhardt, 2022). Essa capacidade abre categorias de negócio anteriormente inviáveis pelos métodos tradicionais como pagamentos por *streaming* de conteúdo, *machine-to-machine payments* na Internet das Coisas e remessas transfronteiriças de valores mínimos sem que as tarifas dos intermediários consumam o valor da transação. É necessário, contudo, reconhecer as limitações operacionais da LN: a necessidade de manter canais com liquidez adequada exige planejamento e capital imobilizado em *Bitcoin*; e, conforme destacam Khan e State (2019), as transações na LN oferecem garantias de segurança teoricamente inferiores às da rede base, orientando sua aplicação preferencial para pagamentos de menor valor.

4.3 ESTUDO COMPARATIVO: *BITCOIN*/*LIGHTNING NETWORK* VERSUS SISTEMAS DE PAGAMENTO BRASILEIROS

Para avaliar a competitividade do *Bitcoin* como meio de pagamento no contexto brasileiro, é necessário confrontar suas características técnicas e econômicas com as dos sistemas atualmente dominantes. O Quadro 2, a seguir, sistematiza essa comparação ao longo de nove dimensões relevantes para a função de meio de troca, abrangendo a rede base do *Bitcoin*, a *Lightning Network*, o PIX e o cartão de crédito.

Quadro 2 – Análise comparativa entre *Bitcoin* (*Layer* 1 e *Lightning Network*), PIX e cartão de crédito.

CRITÉRIO	*BITCOIN* (REDE BASE)	*LIGHTNING NETWORK*	PIX	CARTÃO DE CRÉDITO
Velocidade de liquidação	~10 min por bloco; irreversibilidade recomendada após 6 confirmações (~1h).	Instantânea (~1 segundo).	Instantânea (segundos).	Autorização imediata; liquidação em 1–30 dias.
Custo médio por transação	Variável; pode superar USD 10 em períodos de alta demanda na rede.	Frações de centavo (< USD 0,01).	Gratuito para PF; custo baixo para PJ.	1,5% a 3% sobre o valor para lojistas; anuidade para titular.
Escala (TPS)	~7 TPS.	Virtualmente ilimitada (teórico: milhões de TPS).	~45.000 TPS de pico (BCB, 2023).	~5.000–10.000 TPS (Visa/Mastercard).
Disponibilidade	24/7/365, sem interrupções programadas.	24/7/365; dependente de canais ativos e liquidez da rota.	24/7/365.	24/7 (autorização); liquidação em dias úteis.
Intermediários	Nenhum: rede P2P totalmente descentralizada.	Nenhum em rota direta; nós intermediários possíveis no roteamento.	Banco Central + instituições financeiras participantes.	Emissor, bandeira, adquirente e subadquirente.
Reversibilidade	Irreversível após confirmações suficientes na cadeia.	Irreversível após liquidação e fechamento do canal.	Irreversível; devolução depende da contraparte.	Estorno possível via instituição emissora.
Abrangência geográfica	Global, sem restrições de fronteira ou conversão cambial.	Global.	Restrito ao território brasileiro.	Internacional, com tarifas de câmbio e incidência de IOF.
Privacidade	Pseudônima: transações públicas e rastreáveis no *blockchain.*	Maior privacidade que rede base via *onion routing.*	Identificação obrigatória por chave Pix cadastrada.	Dados completos do titular registrados e acessíveis à operadora.

Fonte: Elaborado pelo autor com base em Nakamoto (2008), Antonopoulos, Osuntokun e Pickhardt (2022), Khan e State (2019), Narayanan *et al*. (2016) e Banco Central do Brasil (2023).

A análise do Quadro 2 evidencia que a rede base do *Bitcoin*, em sua configuração atual, não é competitiva para pagamentos de varejo no contexto brasileiro dimensão em que o PIX apresenta superioridade inequívoca. A velocidade de liquidação do PIX é praticamente instantânea, sem custo para o usuário final pessoa física, com disponibilidade ininterrupta e plena interoperabilidade entre as instituições financeiras do país (Banco Central do Brasil, 2023). Esses atributos respondem de forma eficaz às necessidades da ampla maioria das transações cotidianas realizadas por consumidores e comerciantes brasileiros.

Contudo, a comparação muda substancialmente quando a *Lightning Network* é inserida na análise. Em velocidade e custo por transação, a LN é equivalente ou superior ao PIX: a liquidação é instantânea e as taxas são frações de centavo, viabilizando casos de uso como micropagamentos que o PIX não foi desenhado para atender de forma eficiente. A distinção mais significativa reside nas dimensões de fronteira geográfica e intermediários. Enquanto o PIX é um sistema estritamente nacional e depende da infraestrutura do Banco Central e das instituições financeiras participantes, a *Lightning Network* opera globalmente sem qualquer intermediário centralizado (Antonopoulos; Osuntokun; Pickhardt, 2022).

Essa assimetria posiciona o *Bitcoin*/LN em um nicho competitivo distinto do PIX. Conforme argumenta Ulrich (2014), a principal proposta de valor do *Bitcoin* não é a eficiência transacional per se, mas a resistência à censura e à interferência de terceiros. Para um imigrante enviando remessa ao seu país de origem, para uma empresa realizando pagamento internacional sem a fricção do câmbio bancário tradicional, ou para um indivíduo em um país com controle de capitais, o *Bitcoin*/LN oferece uma alternativa cujo diferencial não pode ser replicado pelo PIX. Do ponto de vista da política monetária, Friedman (2014) demonstrava que a capacidade do governo de controlar a moeda equivale a um poder tributário discricionário exercido via inflação. O *Bitcoin*, com sua política monetária algorítmica e pública, representa o oposto: uma moeda cujas regras de emissão são conhecidas, imutáveis e verificáveis por qualquer participante da rede, atendendo à demanda liberal por "regras, não governamentais".

A dimensão da privacidade também merece atenção. O PIX exige identificação obrigatória do titular via chave cadastrada, tornando cada transação rastreável pelas instituições financeiras e pelo Banco Central. A *Lightning Network*, com seu protocolo de *onion routing*, oferece um grau significativamente maior de privacidade (Khan; State, 2019). Hayek (2011) argumentava que a concorrência entre diferentes formas de dinheiro seria benéfica para a sociedade, pois permitiria que os indivíduos escolhessem a moeda que melhor atendesse às suas necessidades específicas. Sob essa perspectiva, a coexistência do PIX e do *Bitcoin*/LN no ecossistema brasileiro não é uma anomalia, mas uma expressão saudável da diversificação monetária.

4.4 O CENÁRIO REGULATÓRIO BRASILEIRO COMO CONDICIONANTE DA VIABILIDADE DO *BITCOIN* COMO MEIO DE PAGAMENTO

A análise do cenário regulatório brasileiro, conduzida a partir dos documentos normativos levantados na pesquisa, revelou que o principal fator limitante da viabilidade do *Bitcoin* como meio de pagamento no país não é de natureza técnica nem teórica, mas legislativa. Conforme identificado na fundamentação teórica, o Estado brasileiro adotou, desde 2014, uma estratégia de contenção progressiva que não recorre à proibição direta do protocolo algo tecnicamente inviável dada a descentralização da rede, mas atua sobre os intermediários que permitem seu acesso e sobre o tratamento fiscal de cada transação.

O resultado dessa abordagem é um arcabouço normativo que, ao negar ao *Bitcoin* o estatuto de moeda pelo Comunicado BCB nº 25.306/2014, removeu-o do regime de curso forçado e abriu caminho para que a Receita Federal o tratasse como ativo alienável. Essa decisão fundante está diretamente alinhada ao que Mises (1953) identificava como o primeiro mecanismo pelo qual o Estado historicamente protege o monopólio da moeda oficial frente a concorrentes emergentes: a definição jurídica da moeda como prerrogativa exclusiva do poder público, que exclui os demais instrumentos do campo monetário antes mesmo de regular seu uso.

A consequência mais direta e limitante desse posicionamento jurídico foi operacionalizada pela Instrução Normativa RFB nº 1.888/2019, cujos resultados a pesquisa identifica como o obstáculo estrutural mais relevante à função de pagamento do *Bitcoin* no

Brasil. Ao tratar cada utilização do *Bitcoin* para aquisição de bens ou serviços como uma alienação de ativo sujeita à apuração de ganho de capital, a norma criou uma assimetria regulatória sem equivalente nos sistemas de pagamento concorrentes: enquanto o uso do Real, do PIX ou do cartão de crédito não gera qualquer obrigação acessória de apuração para o pagador, cada transação em *Bitcoin* exige o registro do custo de aquisição, o cálculo do ganho proporcional e, se o total de alienações no mês exceder o limite de isenção, o recolhimento do imposto.

Conforme analisado na seção 2.6.2, esse mecanismo transformou as *exchanges* em agentes de fiscalização e inseriu o ecossistema de criptoativos no perímetro de controle da administração tributária nacional. Os resultados da pesquisa evidenciam que esse tratamento fiscal opera como um desincentivo funcional ao uso cotidiano do *Bitcoin* mesmo nos casos em que a *Lightning Network* já seria plenamente competitiva com o PIX em termos de velocidade e custo confirmando, no plano empírico, a análise de Huerta de Soto (2012), para quem o aparato fiscal é o principal instrumento de contenção de instrumentos monetários concorrentes, dispensando qualquer proibição explícita.

A pesquisa revelou ainda que a aprovação do Marco Legal dos Criptoativos, pela Lei nº 14.478/2022, e a subsequente edição das Resoluções BCB nº 519, 520 e 521, vigentes desde fevereiro de 2026, produziram um resultado ambíguo para o ecossistema. Por um lado, ao criar a figura jurídica das Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs) e submetê-las à supervisão do Banco Central, o Marco Legal conferiu legitimidade institucional ao setor, aumentou a confiança dos usuários que operam em plataformas reguladas e introduziu mecanismos de proteção patrimonial como a segregação obrigatória dos recursos dos clientes, determinada pela Resolução BCB nº 520 que reduzem o risco de perdas por insolvência das plataformas.

Por outro lado, ao impor às SPSAVs exigências de capital mínimo, estrutura de governança corporativa, políticas de prevenção à lavagem de dinheiro e padrões de segurança cibernética equivalentes aos das instituições financeiras tradicionais, a regulamentação reproduziu, nos pontos de acesso ao ecossistema de criptoativos, a mesma lógica institucional do sistema financeiro que o *Bitcoin* foi concebido para dispensar. Esse resultado está em conformidade com o que Rothbard (2009) identificava como o processo histórico de absorção regulatória de concorrentes monetários: o Estado não os elimina, mas os doméstica, impondo-lhes os custos de conformidade que garantem sua dependência estrutural do arcabouço institucional vigente.

No que diz respeito à Instrução Normativa BCB nº 704/2026, que implementou a *Travel Rule* com vigência a partir de maio de 2026, a pesquisa identificou o resultado mais expressivo para a dimensão da resistência à censura, que é um dos atributos centrais do *Bitcoin* destacados tanto na proposta original de Nakamoto (2008) quanto na análise de Ulrich (2014). Ao exigir das SPSAVs a identificação completa dos titulares das carteiras de origem e destino em todas as transações, a norma reintroduziu, no plano das interfaces reguladas de acesso ao ecossistema, o requisito de confiança em um terceiro que o sistema *peer-to-peer* foi projetado para eliminar.

Conforme descrito na seção 2.6.4, esse alinhamento às recomendações internacionais do Grupo de Ação Financeira Internacional (GAFI) representa a convergência mais explícita entre o ecossistema cripto e o sistema financeiro convencional no Brasil. Os resultados indicam que a *Travel Rule* delimita, na prática, dois regimes distintos de uso do *Bitcoin* no país: o regime das plataformas supervisionadas, que oferece proteção institucional ao custo da rastreabilidade plena e da identificação obrigatória; e o regime de auto custódia via *Lightning Network*, que preserva os atributos de privacidade e resistência à censura do protocolo, mas mantém as obrigações fiscais sobre ganho de capital da IN RFB nº 1.888/2019.

Essa bifurcação confirma que a estratégia regulatória brasileira foi eficaz em capturar o ecossistema intermediado sem precisar proibir o uso direto do protocolo.

A análise integrada dos resultados legislativos permite, por fim, responder ao quarto objetivo específico desta pesquisa examinar o cenário jurídico-regulatório brasileiro para criptoativos e conectar esse achado à pergunta de pesquisa central. Os resultados demonstram que o arcabouço normativo construído entre 2014 e 2026 opera de forma sistêmica: a exclusão monetária pelo Comunicado BCB nº 25.306/2014 fundou o regime tributário; a IN RFB nº 1.888/2019 operacionalizou a penalização fiscal de cada transação; o Marco Legal e as Resoluções BCB nº 519, 520 e 521 institucionalizaram os intermediários sob padrões equivalentes aos do sistema financeiro; e a *Travel Rule* estendeu a rastreabilidade plena ao ecossistema regulado.

Cada instrumento reforçou o anterior, compondo uma estrutura de controle que não precisa proibir para ser eficaz. Esse resultado confirma a observação de Hayek (2011) sobre a relação histórica entre Estado e moeda: os governos não precisam eliminar os concorrentes monetários para proteger o monopólio da moeda oficial; basta regulá-los de forma assimétrica, impondo sobre eles os ônus que a moeda oficial não carrega. No caso brasileiro, a legislação analisada cumpriu exatamente essa função, condicionando a viabilidade do *Bitcoin* como meio de pagamento não à tecnologia disponível, mas às escolhas normativas do Estado.

5 CONSIDERAÇÕES FINAIS

Este trabalho buscou responder à seguinte pergunta de pesquisa: qual a viabilidade, sob as óticas de execução, base teórica e regulatória, do *Bitcoin* como meio de pagamento no Brasil? Para respondê-la, a pesquisa percorreu quatro dimensões interdependentes: expor a teoria da Escola Austríaca sobre a natureza da moeda como base analítica, analisar o protocolo Bitcoin como solução tecnológica para a desestatização do dinheiro, comparar a execução de pagamentos via *Bitcoin* e *Lightning Network* com os principais sistemas disponíveis no Brasil e examinar o cenário jurídico-regulatório brasileiro para criptoativos. A integração dessas dimensões permite afirmar, com base nos resultados obtidos, que o *Bitcoin* é tecnicamente viável como meio de pagamento no Brasil.

Do ponto de vista técnico, a *Lightning Network* demonstrou que os gargalos históricos da rede base velocidade, custo e capacidade de escala foram resolvidos em nível de protocolo, tornando o *Bitcoin* competitivo com sistemas como o PIX para transações de baixo valor. Do ponto de vista teórico, o *Bitcoin* satisfaz de forma robusta os critérios monetários da Escola Austríaca, superando o padrão histórico do ouro em portabilidade, divisibilidade e resistência à manipulação estatal, e realizando em código o ideal de dinheiro sólido preconizado por Mises (1953), Hayek (2011) e Rothbard (2013). A qualificação teórica e técnica do *Bitcoin* como candidato à função de meio de troca é, portanto, sólida.

Contudo, os resultados da pesquisa evidenciam que essa viabilidade técnica e teórica não se traduz, no contexto brasileiro atual, em uma recomendação prática de uso cotidiano como substituto da moeda fiduciária. O arcabouço legislativo analisado da exclusão monetária pelo Comunicado BCB nº 25.306/2014 ao tratamento tributário da IN RFB nº 1.888/2019, passando pelas Resoluções BCB nº 519, 520 e 521/2025 e pela *Travel Rule* da IN BCB nº 704/2026 impõe sobre cada transação em *Bitcoin* obrigações fiscais e custos de conformidade que inexistem para o uso do Real. Esse atrito normativo é o principal fator limitante à adoção do *Bitcoin* como meio de troca geral no Brasil, confirmando a análise de Huerta de Soto (2012) sobre o papel da regulação assimétrica na proteção do monopólio monetário estatal.

Um achado central desta pesquisa é que a dificuldade de adoção do *Bitcoin* como meio de troca cotidiano não representa uma falha do protocolo, mas uma consequência direta

de suas qualidades monetárias superiores. A teoria econômica austríaca, especialmente na formulação de Rothbard (2013), identificou que quando duas formas de moeda coexistem em uma mesma economia, os agentes tendem a gastar a moeda de menor qualidade e a reter a de maior qualidade fenômeno conhecido como Lei de Gresham. O Real, como moeda fiduciária sujeita à emissão discricionária e à erosão inflacionária, configura o que a Escola Austríaca denomina moeda fraca: seu valor se deteriora ao longo do tempo, criando o incentivo de convertê-lo em bens ou ativos antes que perca poder de compra.

O *Bitcoin*, por sua vez, com oferta limitada a 21 milhões de unidades e política monetária imutável, configura uma reserva de valor de primeira ordem, cujo poder de compra histórico tem demonstrado tendência de apreciação no longo prazo. O resultado prático dessa assimetria é que o usuário que possui ambos os ativos tendem naturalmente a gastar o Real e a conservar o *Bitcoin*, não por irracionalidade, mas por pura lógica econômica. Nesse sentido, é mais recomendável, no contexto brasileiro atual, que o usuário utilize a moeda fiduciária para as transações do dia a dia e o *Bitcoin* como reserva de valor de longo prazo, protegendo parte do patrimônio da erosão inflacionária que a moeda fraca inevitavelmente impõe ao longo do tempo, conforme alertavam Mises (2010) e Friedman (2014).

Isso não significa, porém, que o *Bitcoin* seja inviável como meio de pagamento em todos os contextos. Os resultados apontam que, para pagamentos internacionais, remessas transfronteiriças e micropagamentos programáticos, o *Bitcoin* via *Lightning Network* apresenta diferenciais concretos e insubstituíveis: ausência de intermediários, disponibilidade permanente, custo próximo de zero e alcance global sem conversão cambial. Nesses casos específicos, os diferenciais técnicos superam os obstáculos fiscais envolvidos e justificam seu uso como meio de troca, mesmo no atual cenário regulatório brasileiro. A viabilidade do *Bitcoin* como meio de pagamento é, portanto, seletiva e contextualmente determinada.

Esta pesquisa apresenta contribuições tanto teóricas quanto práticas. Do ponto de vista teórico, demonstrou que as categorias analíticas da Escola Austríaca são plenamente aplicáveis à análise de um ativo digital descentralizado, permitindo avaliar o *Bitcoin* como candidato legítimo à função monetária em sua acepção mais fundamental. Do ponto de vista prático, oferece a gestores, empreendedores e formuladores de políticas públicas uma síntese dos fatores que condicionam a adoção do *Bitcoin* no Brasil. Como limitações, o estudo reconhece que se baseou exclusivamente em fontes secundárias e que o cenário regulatório e tecnológico do setor evolui com velocidade elevada as próprias Resoluções BCB nº 519, 520 e 521, analisadas neste trabalho, entraram em vigor durante o período de elaboração da pesquisa, o que pode alterar parte das conclusões em horizonte relativamente curto. Para pesquisas futuras, sugere-se a realização de estudos empíricos com usuários e comerciantes que já adotam o *Bitcoin* como meio de pagamento no Brasil, bem como análises comparativas com países que avançaram em modelos regulatórios mais favoráveis à sua função transacional como El Salvador, cujo experimento de adoção como moeda de curso legal desde 2021 oferece dados concretos ainda pouco explorados pela literatura nacional, e o monitoramento do impacto da *Travel Rule* sobre o volume de transações em *exchanges* supervisionadas a partir de maio de 2026.

REFERÊNCIAS

ANTONOPOULOS, Andreas M. **Mastering Bitcoin***:* programming the open blockchain. 2. ed. Sebastopol, CA: O'Reilly Media, 2017.

ANTONOPOULOS, Andreas M.; OSUNTOKUN, Olaoluwa; PICKHARDT, Rene. **Mastering the Lightning Network:** A Second Layer Blockchain Protocol for Instant Bitcoin

Payments. Sebastopol: O'Reilly Media, 2022.

BRASIL. Banco Central do Brasil. **Estatísticas de meios de pagamento**. Brasília, DF: Banco Central do Brasil, 2023.

BRASIL. Banco Central do Brasil. **Instrução Normativa BCB nº 704, de 2026**. Estabelece procedimentos e leiautes para remessa de informações relativas às sociedades prestadoras de serviços de ativos virtuais. Brasília, DF: Banco Central do Brasil, 2026. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Instru%C3%A7%C3%A3o%20Normativa%20BCB&numero=704. Acesso em: 6 mai. 2026.

BRASIL. Banco Central do Brasil. **Relatório de Vigilância do Sistema de Pagamentos Brasileiro**. Brasília, DF: Banco Central do Brasil, 2014.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 1, de 12 de agosto de 2020**. Institui o arranjo de pagamentos Pix e aprova o seu Regulamento. Brasília, DF: Banco Central do Brasil, 2020. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=1. Acesso em: 30 ago. 2025.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 519, de 10 de novembro de 2025**. Disciplina o processo de autorização para funcionamento das sociedades prestadoras de serviços de ativos virtuais. Brasília, DF: BCB, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=519. Acesso em: 7 mar. 2026.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 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: BCB, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=520. Acesso em: 7 mar. 2026.

BRASIL. Banco Central do Brasil. **Resolução BCB nº 521, de 10 de novembro de 2025**. Dispõe sobre alterações em normas do mercado de câmbio e prestação de serviços de ativos virtuais. Brasília, DF: BCB, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=521. Acesso em: 7 mar. 2026.

BRASIL. Banco Central do Brasil. **Comunicado nº 25.306, de 19 de fevereiro de 2014**. Esclarece sobre os riscos decorrentes de operações com as denominadas "moedas virtuais". Brasília, DF: BCB, 2014. Disponível em: https://www.google.com/search?q=https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo%3Ftipo%3DComunicado%26numero%3D25306. Acesso em: 4 set. 2025.

BRASIL. Comissão de Valores Mobiliários. **Parecer de Orientação CVM nº 40, de 11 de outubro de 2022**. Dispõe sobre a oferta de Tokens de Recebíveis ou de Renda Fixa (“Tokens de Renda Fixa”), no contexto das ofertas públicas de valores mobiliários dispensadas de registro. Rio de Janeiro: CVM, 2022b. Disponível em: https://www.google.com/search?q=https://conteudo.cvm.gov.br/legislacao/pareceres-orientacao/par-ori040.html. Acesso em: 4 set. 2025.

BRASIL. **Lei nº 4.595, de 31 de dezembro de 1964**. Dispõe sobre a Política e as Instituições Monetárias, Bancárias e Creditícias, cria o Conselho Monetário Nacional e dá outras providências. Brasília, DF: Presidência da República, 1964. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l4595.htm. Acesso em: 4 set. 2025.

BRASIL. Presidência da República. **Lei nº 14.478, de 21 de dezembro de 2022**. Dispõe sobre diretrizes a serem observadas na prestação de serviços de ativos virtuais e na regulamentação dos prestadores de serviços de ativos virtuais [...]. Brasília, DF: Presidência da República, 2022a. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/l14478.htm. Acesso em: 4 set. 2025.

BRASIL. Secretaria Especial da Receita Federal do Brasil. **Instrução Normativa RFB nº 1.888, de 03 de maio de 2019**. Institui e disciplina a obrigatoriedade de prestação de informações relativas às operações realizadas com criptoativos à Secretaria Especial da Receita Federal do Brasil (RFB). Brasília, DF: RFB, 2019. Disponível em: https://www.google.com/search?q=http://normas.receita.fazenda.gov.br/sijut2consulta/link.action%3Fvisao%3Danotado%26idAto%3D100574. Acesso em: 4 set. 2025.

BUDISH, E. **The Economic Limits of Bitcoin and the Blockchain.** NBER Working Paper, n. 24717, 2018.

COURTOIS, Nicolas T.; GRAJEK, Marek; NAIK, Rahul. **The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining.** In: INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY, 18., 2014, Christ Church. Proceedings**...** Berlin: Springer, 2014. p. 104-121.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 3. ed. Porto Alegre: Artmed, 2010.

FRIEDMAN, Milton. **Capitalismo e Liberdade**. São Paulo: LVM, 2014.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 7. ed. Barueri, SP: Atlas, 2022.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

HAYEK, Friedrich A. **Desestatização do dinheiro**: uma análise da teoria e prática das moedas simultâneas. 2. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2011.

HÜLSMANN, Jörg Guido. **The Ethics of Money Production.** Auburn: Ludwig von Mises Institute, 2008.

HUERTA DE SOTO, Jesús. **Moeda, crédito bancário e ciclos econômicos**. São Paulo: Instituto Ludwig von Mises Brasil, 2012.

KHAN, Nida; STATE, Radu. **Lightning Network**: A Comparative Review of Transaction Fees and Data Analysis. Luxembourg: University of Luxembourg, 2019.

KROLL, Joshua A.; DAVEY, Ian C.; FELTEN, Edward W. **Bitcoin in the Presence of Adversaries**. In: THE TWELFTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS 2013), 2013, Washington, DC. Anais... Washington, DC: WEIS, 2013. p. 1-21.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de metodologia científica**. 5. ed. São Paulo: Atlas, 2003.

MENGER, Carl. **On the origins of money**. Economic Journal, v. 2, n. 6, p. 239-255, 1892.

MISES, Ludwig von. **Ação Humana**: um tratado de economia. 3. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2010.

MISES, Ludwig von. **The theory of money and credit**. New Haven: Yale University Press, 1953.

NAKAMOTO, Satoshi. **Bitcoin***:* a Peer-to-Peer Electronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 4 set. 2025.

NARAYANAN, Arvind *et al*. **Bitcoin and cryptocurrency technologies**: a comprehensive introduction. Princeton: Princeton University Press, 2016.

ROTHBARD, Murray N. **Man, Economy, and State with Power and Market**. 2. ed. Auburn: Ludwig von Mises Institute, 2009.

ROTHBARD, Murray N. **The Mystery of Banking**. 2. ed. Auburn: Ludwig von Mises Institute, 2008.

ROTHBARD, Murray N. **O que o governo fez com o nosso dinheiro?** São Paulo: Instituto Ludwig von Mises Brasil, 2013.

SMITH, Adam. **A Riqueza das Nações**: Investigação sobre sua Natureza e suas Causas. v. I. São Paulo: Nova Cultural, 1996. (Coleção Os Economistas).

TUCKER, Jeffrey. Prefácio. In: ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

ULRICH, Fernando. **Bitcoin**: a moeda na era digital. São Paulo: Instituto Ludwig von Mises Brasil, 2014.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 2. ed. São Paulo: Atlas, 1998.

WARREN, Micah. **Bitcoin: A Game-Theoretic Analysis.** Berlin: De Gruyter, 2023.

YANO, Makoto *et al*. (ed.). **Blockchain and Crypt Currency***: Building a High Quality Marketplace for Crypt Data*. Singapore: Springer, 2020.