UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE ECONOMIA
BACHARELADO EM CIÊNCIAS ECONÔMICAS

LUCAS DOS SANTOS BARBOSA

Bitcoin: soberania financeira ou armadilha fiduciária?

RECIFE — PE

2023

LUCAS DOS SANTOS BARBOSA

Bitcoin: soberania financeira ou armadilha fiduciária?

Trabalho de Conclusão de Curso apresentado pelo aluno **Lucas dos Santos Barbosa** ao Curso de Ciências Econômicas da Universidade Federal Rural de Pernambuco — UFRPE, como pré-requisito parcial para a obtenção do grau de Bacharel em Ciências Econômicas sob a orientação do professor **Dr. Luís Eduardo Barbosa Carazza**.

RECIFE — PE

2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

B238b Barbosa, Lucas dos Santos
Bitcoin: soberania financeira ou armadilha fiduciária? / Lucas dos Santos Barbosa. - 2023.
69 f. : il.

Orientador: Luis Eduardo Barbosa Carazza.
Inclui referências.

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal Rural de Pernambuco, Bacharelado em Ciências Econômicas, Recife, 2024.

1. Bitcoin. 2. Fiduciário. 3. Centralização. 4. Autocustódia. I. Carazza, Luis Eduardo Barbosa, orient. II. Título

CDD 330

Monografia apresentada como requisito necessário para a obtenção do título de Bacharel em Ciências Econômicas. Qualquer citação atenderá as normas da ética científica.

Bitcoin: soberania financeira ou armadilha fiduciária?

LUCAS DOS SANTOS BARBOSA

Trabalho de Conclusão de Curso aprovado com nota _____ apresentado em ____/ ____/ ____

BANCA EXAMINADORA

_____
Orientador. Prof. Dr. Luís Eduardo Barbosa Carazza

_____
1º Examinador. Prof. Dr. Álvaro Furtado Coelho Júnior

_____
2º Examinador. Prof. Dr. André de Souza Melo

AGRADECIMENTOS

Meu pai, Sebastião Barbosa, que faleceu durante a minha jornada universitária, mas que certamente permaneceu me dando forças diariamente. Seus conselhos e ensinamentos estarão sempre comigo.

Minha mãe, Fabiola, cujo apoio inabalável foi a âncora que me sustentou durante os períodos de dificuldade.

Aos excelentes companheiros que a UFRPE me concebeu: Marianna Carvalho, Renato Lopes, Marcos Vieira, Sebastião Júnior e Álvaro Martínez. Amizades e parcerias que tornaram os anos acadêmicos mais alegres.

Ao professor Luis Carazza, pelo conhecimento e orientação que me concebeu desde a sala de aula até a elaboração desta monografia. Sua dedicação e influência contribuíram para o meu desenvolvimento acadêmico.

À Universidade Federal Rural de Pernambuco, que proporcionou oportunidade, estrutura, acomodação e excelentes profissionais da educação na minha formação.

RESUMO

O Bitcoin busca desafiar o sistema fiduciário resolvendo diversos problemas associados ao modelo centralizado. Porém, inúmeros problemas de escalabilidade são verificáveis devido a capacidade limitada de processamento da *blockchain*. Diante disso, os usuários buscam novas alternativas para a criptomoeda, e a *Lightning Network* (*LN*) surge como uma solução que proporciona transações rápidas e econômicas. No entanto, a *LN* é fortemente centralizada e controlada por poucas entidades, suscitando em preocupações sobre privacidade, segurança, modificações tarifárias e regulamentações governamentais. Outra abordagem popular é a negociação de contratos de Bitcoins em corretoras, bancos, instituições de pagamento e empresas de carteiras custodiais. Embora mais cômodo, esse método acarreta desafios relacionados à privacidade e reserva fracionária. Conclui-se que as estas formas convencionais de utilização do Bitcoin são contrárias às premissas propostas no *whitepaper* e estão conduzindo a moeda para uma forma de moeda fiduciária. Diante deste panorama, a conscientização dos usuários sobre os benefícios do Bitcoin de forma descentralizada é necessária, estimulando a prática de transações *peer-to-peer* (*P2P*) e do armazenamento em autocustódia.

PALAVRAS-CHAVE: Bitcoin; Fiduciário; Centralização; Autocustódia.

ABSTRACT

The Bitcoin attempts to challenge the fiduciary system by solving various problems associated with the centralized model. However, due to the blockchain's limited processing capacity, scalability issues abound. As a result, users are exploring alternative options to Bitcoin, including the Lightning Network (LN), a solution that offers fast and economical transactions. However, the Lightning Network is highly centralized and controlled by a handful of entities, raising concerns about privacy, security, rate adjustments, and government regulation. An alternative and popular approach is to engage in Bitcoin contracts through brokers, banks, payment institutions, and custodial wallet companies. While this method is more convenient, it raises privacy and fractional reserve issues. It is concluded that these applications of bitcoin contradict the principles outlined in the white paper and push the currency towards a fiat money model. In light of this, it is necessary to educate users about the benefits of using bitcoin in a decentralized way, encouraging the practice of peer-to-peer (P2P) transactions and self-custody storage.

KEYWORDS: Bitcoin; Fiduciary; Centralization; Self-custody.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Ao longo da evolução histórica, a percepção da moeda foi além de sua função primária como meio de troca, adquirindo diversos aspectos econômicos fundamentais para as sociedades. Na perspectiva monetária de Rothbard (2013), o dinheiro é o meio que possibilita todas as transações, e por isso, é como o sangue de todo o sistema econômico. Entretanto, a produção e administração do dinheiro são comumente delegadas às autoridades estatais, que possuem o monopólio do poder econômico e administrativo sobre as nações. Portanto, o controle monetário confere aos estados uma das principais ferramentas de controle sobre os indivíduos.

Na contemporaneidade, a estrutura do sistema monetário é reconhecida como sistema fiduciário ou sistema *fiat*. Esse paradigma monetário fundamenta-se na confiança atribuída às autoridades monetárias para orientar as políticas monetárias e preservar o poder de compra em suas áreas de jurisdição (Hayek, 2011). De modo a exemplificar, o Banco Central do Brasil (BACEN) classifica que seu principal objetivo é de “garantir a estabilidade do poder de compra da moeda, zelar por um sistema financeiro sólido, eficiente e competitivo, e fomentar o bem-estar econômico da sociedade”.[1] Assim, grande parte das moedas em circulação, como o dólar americano, o euro e o real, são consideradas moedas fiduciárias.

Antigamente, muitos países adotavam o padrão-ouro, onde o valor da moeda era diretamente vinculado a uma quantidade específica do metal. Entretanto, o lastro foi gradualmente abandonado por lideranças globais, principalmente na década de 70, devido a várias razões, incluindo a necessidade de flexibilidade na política monetária para estimular o crescimento econômico por meio de autofinanciamento governamental. Assim, o atual sistema de moeda *fiat* depende da estabilidade econômica e da confiança das pessoas nas instituições governamentais para manter seu valor, não mais por lastro em ouro.

Com isso, a literatura econômica destaca uma série de desafios e problemas inerentes ao sistema fiduciário, derivado das fortes emissões de moeda para subsídio governamental, que tende a implicar em episódios de

[1] Disponível em: https://www.bcb.gov.br/acessoinformacao/institucional. Acesso em 20, nov. 2023.

crises inflacionárias e a perda de poder de compra. Para Rothbard (2013), a introdução dos governos no controle monetário, em especial com a introdução do sistema completamente fiduciário, contribui para a destruição da produtividade do mercado competitivo e o surgimento de novas guerras bélicas e econômicas entre nações.

Diante desses desafios, uma variedade de atores sociais, entusiastas de uma sociedade mais livre, buscam fundamentar teorias e práticas alternativas ao sistema *fiat*, almejando uma sociedade menos vinculada à moeda governamental. Nesse cenário, o desenvolvimento da tecnologia de criptografia computacional vem desempenhando um papel crucial na viabilização de moedas digitais alternativas (Ammous, 2018). A função criptográfica é útil pois atua um lastro matemático pré-definido que busca impedir o controle monetário, inclusive da emissão.

Neste âmbito, destaca-se o Bitcoin (BTC), sendo a primeira implementação bem-sucedida de uma criptomoeda descentralizada, publicada em formato de artigo, denominado *whitepaper*, em outubro de 2008.[2] Há uma curiosa simultaneidade do período em que foi publicado o projeto com a crise financeira em 2008 nos Estados Unidos, situação que incrementa o debate público acerca da perspectiva de economia monetária moderna mais livre.

O Bitcoin pode ser interpretado como uma contraposição ao sistema fiduciário por ser uma moeda livre, ausente de controle governamental ou de poucos indivíduos, contendo um robusto sistema de emissão monetária previamente estabelecido, resguardado por sua tecnologia criptográfica. Assim, diferentemente da moeda *fiat*, não haveria problemáticas derivadas do autofinanciamento do proprietário por processo de emissão.

No entanto, com o aumento da popularidade do Bitcoin, surge um desafio significativo: a escalabilidade de seu uso. As estatísticas de desempenho da *blockchain* (rede do Bitcoin), responsável pela validação e registro das transações, indicam sérios problemas operacionais, tais como instabilidade no sistema, tempo de confirmação de transações prolongado e custos elevados. Embora essas questões não sejam necessariamente obstáculos significativos para o uso da moeda como reserva de valor, tornam a utilização como meio de

[2] Disponível em: https://bitcoin.org/bitcoin.pdf

troca para microtransações praticamente inviável. Como resultado, empresas e desenvolvedores independentes buscam alternativas para resolver esses problemas, incluindo a realização de transações em plataformas alternativas e elaborações de redes paralelas, conhecidas como soluções de segunda camada.

Uma alternativa de segunda camada amplamente adotada é a *Lightning Network* (*LN*), que se apresenta como uma solução promissora para viabilizar transações mais rápidas e econômicas utilizando o Bitcoin. De acordo com as estatísticas de utilização dessa rede alternativa, o tempo de confirmação das transações é praticamente instantâneo, enquanto os custos de transação são quase insignificantes (Antonopoulos; Osuntokun e Pickhardt, 2022). Essas características tornam a *LN* uma alternativa altamente atrativa, e sua adoção está crescendo significativamente.

Uma alternativa para negociar Bitcoin segue o padrão de contratos, semelhante do utilizado no mercado financeiro para transações de comodities. Diversas instituições de pagamentos, corretoras, e bancos estão entrando no mercado de criptomoeda e oferecem serviços de compra, venda e custódia desse ativo. A busca por essa alternativa se fundamenta devido à simplicidade relativa dessas alternativas e à sua integração no mesmo ambiente das finanças convencionais.

No entanto, diante de todo este cenário, questões críticas acerca das funções existenciais do Bitcoin podem surgir. Supondo que, majoritariamente, seja adotada pelos indivíduos que as negociações deste ativo ocorram em plataformas centralizadas, havendo menos interesse nas negociações na *blockchain*, essas soluções violariam os princípios fundamentais Bitcoin enquanto uma alternativa ao sistema *fiat*? Estaria, nesse cenário, o Bitcoin se tornando mais uma ferramenta fiduciária?

Os objetivos gerais desta pesquisa são de investigar se há, de fato, processos em curso que resultam na transformação do Bitcoin em uma moeda mais centralizada e controlada por determinadas entidades públicas ou privadas. E, caso positivo, destacar as formas que isto ocorre, os principais riscos, e provocar discussões por alternativas funcionais ao Bitcoin que mantém os princípios originários.

Os objetivos específicos incluem compreender o desenvolvimento da moeda convencional ao longo da história, sua natureza adaptativa e os desafios enfrentados no sistema fiduciário. Em um segundo momento, identificar o Bitcoin como uma alternativa monetária descentralizada e suas limitações em termos de escalabilidade. Posteriormente, destacar algumas alternativas para a problemática, como a utilização da *Lightning Network* e a negociação de contratos de Bitcoins em corretoras e instituições bancárias. Por fim, evidenciar os possíveis riscos associados nessas modalidades, propondo uma discussão acerca de alternativas de preservação dos fundamentos do Bitcoin.

Os objetivos delineados nesta pesquisa devem ser alcançados por meio de uma metodologia fundamentada em abordagens científicas sistemáticas, conforme preconizado por Gil (2002). A presente investigação se configura como um estudo de natureza bibliográfica, pautado por uma base teórica abrangente, sustentada por análises críticas de livros e publicações científicas acessíveis nos principais repositórios digitais. Essa abordagem assegura a fundamentação das discussões, contribuindo para a qualidade e rigor metodológico do presente trabalho.

A pesquisa bibliográfica desempenhou um papel fundamental na reconstrução da trajetória histórica da moeda ao longo da história humana. Elucidando as problemáticas do sistema monetário, destacaram-se renomados autores críticos da economia moderna, como Mises, Rothbard e Hayek. Foram utilizados como fontes secundárias sítios virtuais especializados em dados, como *ycharts*, *look into bitcoin*, e Banco Central do Brasil. Essas escolhas proporcionaram informações que fundamentaram a pesquisa suficientemente.

Por fim, a pesquisa contém uma seção argumentativa que destaca as principais evidências encontradas, além de atribuir comentários sobre os riscos de ineficácia do Bitcoin enquanto uma alternativa monetária descentralizada.

2 A NATUREZA MONETÁRIA

A moeda surgiu de forma espontânea, como solução para as limitações do sistema de escambo, o qual era ineficiente para atender às crescentes demandas de uma sociedade mercantil. A negociação por escambo requer a existência de uma dupla coincidência de desejos entre os negociantes, situação que limita as possibilidades de troca e aumenta os custos de transação (Rothbard, 2013). Por exemplo, se um pescador tem interesse em adquirir algodão, mas só possui algumas unidades de peixe fresco para transacionar, é necessário que produtor de algodão tenha interesse nesse pescado e se sinta satisfeito com a troca. Pelo contrário, o pescador deve buscar outro produtor de algodão com esse interesse, situação que custa tempo e esforço significativo. Portanto, é extremamente difícil haver um comércio desenvolvido baseado unicamente em escambo.

A utilização de uma ferramenta de troca indireta dispensa a necessidade dessa dupla coincidência de desejo dos bens transacionados pelos indivíduos. Nesse caminho, a utilização de uma moeda em comum se fez eficaz, e promoveu maior flexibilidade, escalabilidade e produtividade nas transações comerciais, fatores cruciais no desenvolvimento econômico e social a partir da primeira revolução agrícola (Lopes e Rossetti, 2005). Em suma, a moeda permite um maior nível de prosperidade econômica e riqueza para as sociedades.

À priori, é necessário definir quais são os elementos essenciais para caracterizar algo como moeda, especialmente devido às diversas faces adquiridas por ela ao longo das eras. De acordo com Gremaud (2004), a classificação monetária se baseia em três funções fundamentais: ser um meio de troca, uma unidade de conta e uma reserva de valor. Portanto, independentemente da ferramenta utilizada como moeda, essas três funções devem se fazer presentes.

A função de meio de troca é a própria lógica da origem da moeda, sendo necessária para a realização de transações eficientes, alheia aos itens envolvidos diretamente na comercialização que permeia o sistema de escambo. Segundo Rothbard (2013), a função de meio de troca é a principal maneira que a moeda pode emergir e se estabelecer como uma alternativa de uso para os agentes econômicos. Sendo assim, os itens definidos como moeda por alguma

autoridade monetária podem não performar eficientemente na sociedade caso estes não sejam valorados pelos indivíduos.

A unidade de conta é função de quantificação monetária dos bens e serviços transacionados na economia. Por exemplo, a informação de quantos dólares são necessários para obter um determinado carro, ou, quantos reais são necessários para comprar um novo laptop. Na interpretação de Metri (2012), essa é a característica fundamental que uma moeda deve possuir, mais importante que a função de meio de troca ou reserva de valor.

A função de reserva de valor é capacidade de manter a moeda em custódia ao longo do tempo, preservando a riqueza do indivíduo que decidiu poupar. Nessa perspectiva, a moeda permite ao indivíduo a capacidade de armazenar dinheiro, dispensando o uso imediato e permitindo acumulando riqueza para o consumo futuro (Aggio, 2008). Para que isso ocorra, a moeda escolhida deve ter seu poder de compra estável ao longo do tempo, pelo contrário, não haveria incentivos a poupar.

Além das funções supracitadas, as características de fungibilidade, portabilidade, durabilidade e divisibilidade são definidas como necessárias para uma moeda ter boa aceitação na economia (Aristotle, 1994). A fungibilidade diz respeito a homogeneidade do bem, em quantidade e qualidade, podendo haver a substituição de uma unidade por outra sem prejuízo monetário. A portabilidade requer que haja a possibilidade de a moeda ser transportada de um local para outro sem prejuízos oriundos do seu volume ou tamanho. A durabilidade é fundamental, pois, sendo a moeda um meio de troca, será repassada por diversos indivíduos constantemente, e sua qualidade deve ser a mais duradoura possível. Por fim, a divisibilidade se traduz na capacidade de dividir a moeda em pequenas frações unitárias, permitindo que haja negociação de produtos e serviços de menor valor utilizando a mesma.

2.1 A MOEDA MERCADORIA

As moedas iniciais assumiam as características de mercadorias comuns, divergindo completamente da faceta visualizada nos tempos contemporâneos. Denominadas de moedas-mercadorias, diferentes bens foram utilizados ao longo do tempo, tais como animais, trigo, café, sal e cigarros

(Reverter, 2020). O gado, por exemplo, em diversas sociais foi um dos bens mais valorados nos comércios (Ammous, 2018). Aspectos como valor nutricional enquanto alimento e aspectos de mobilidade podem justificar essa busca.

Um dos requisitos essenciais para um bem ser determinado como moeda é a sua alta demanda no mercado. Este deve ser útil e valorizado por si só, independentemente de sua função monetária (Rothbard, 2013). Por isso, seu valor também é fruto das suas propriedades naturais enquanto mercadoria, que garantem aceitação em futuras transações.

Embora as moedas-mercadoria se firmaram como alternativas mais eficientes que o sistema de escambo, o uso diário ainda se mostrou limitado em diversos aspectos. O principal desafio surgiu com o desenvolvimento tecnológico e produtivo das economias, que resultou em uma maior eficiência na produção de bens e serviços, permitindo que novas “unidades monetárias” sejam criadas (Ammous, 2018). Por exemplo, o tabaco sendo utilizado como moeda, grandes são os incentivos para o seu cultivo em larga escala. Com isso, investimentos em melhores técnicas agrícolas são realizadas para melhorar a eficiência nas plantações. Por resultado, há um incremento na produtividade, desencadeando um processo de excesso de oferta monetária. Em suma, tornou-se cada vez mais necessária a adoção de uma ferramenta monetária de alto custo produtivo e com características naturais valorizadas pela sociedade que a utilizará.

Os metais se destacaram ao longo do tempo por apresentarem diversos benefícios em contraste com os bens previamente utilizados. Os principais ganhos são de facilidade de armazenamento, eliminação da perecibilidade, maior divisibilidade e a capacidade de fusão (Smith, 1996). Essas características são preferíveis ao conceito de moeda baseado na metafísica monetária aristotélica citada anteriormente.

A facilidade de armazenamento ocorre, pois, ao utilizar uma peça de metal cunhada e padronizada, a riqueza pode ser expressa em um pequeno objeto de fácil manuseio. A eliminação da perecibilidade também é vantajosa, dispensando enormes custos de manutenção de estoque. A possibilidade de divisão e fusão permite que a riqueza seja fracionada ou unificada, resolvendo problemas logísticos e possibilitando transações comerciais com pequenos objetos cunhados. Portanto, são diversos os benefícios da adoção desta nova

modalidade monetária em comparação com o sistema anterior. Pode-se observar, conforme Figura 1, alguns itens utilizados como moeda metálica ao longo da história, como facas, chaves, moedas e lingotes de ouro.

Figura 1 — Metais precisos como moeda

Fonte: Banco Central do Brasil, 2004. Adaptado pelo autor.

As primeiras moedas metálicas eram feitas de metais não preciosos, como bronze e ferro, de alta abundância natural. Como resultado, a relação entre estoque e fluxo foi comprometida, tornando-as inadequadas para uso a longo prazo. A solução para esse problema foi a adoção generalizada por moedas feitas de ouro, prata e cobre, que eram suficientemente raras para garantir a estabilidade dos preços na economia (Lopes e Rossetti, 2005).

A produção das moedas metálicas é denominada de cunhagem, e esse processo foi iniciado pelo Rei Creso da Lídia no século VI a.C (Hayek, 2011). Entretanto, outras fontes arqueológicas apontam que o surgimento ocorreu durante a Dinastia Chou, na China, também no século VI a.C (Ibrachina, 2023). Em ambos os casos, o Estado tornou-se responsável pela qualidade e pureza das moedas cunhadas, mediante uma taxa — denominada senhoriagem — que serviu de autofinanciamento para os impérios (Rothbard, 2013). Nesse sentido, o Império Romano tomou gradualmente o controle da cunhagem ao longo do tempo, enquanto a China imperial proibiu completamente a produção privada em 186 a.C. (Reverter, 2020). Com a renda da senhoriagem, os estados obtiveram maior poder econômico, obtendo capacidade de adquirir mais produtos e serviços e aumento de gastos para recursos militares, sem a necessidade de incrementar o nível de impostos de forma direta.

A introdução do controle estatal da cunhagem e a padronização da moeda metálica trouxeram consigo várias vantagens iniciais para a população. Conforme argumentado por Hayek (2011), essa iniciativa permitiu que os indivíduos se familiarizassem com o uso de uma única moeda como unidade de conta, além de garantir um pequeno ganho na autenticidade da pureza da moeda. A uniformização monetária, com a padronização dos preços em uma moeda principal, resultou em um ganho significativo de eficiência de mercado. Além disso, devido à dificuldade de avaliar com precisão a pureza de cada moeda metálica, a verificação em larga escala realizada pelo estado contribuiu para um aumento na eficiência do mercado.

Todavia, Hayek (2011) afirma que esses ganhos não superam os problemas oriundos da centralização da cunhagem da moeda metálica. Corroborando com Rothbard, a visão de Hayek (2011) era de que a moeda passou a ser utilizada como instrumento de poder e autofinanciamento estatal, sendo a cunhagem uma das principais fontes de renda o império romano. Diante disso, as motivações iniciais de padronização monetária para ganhos sociais se mostraram como apenas narrativa para aumento de poder.

Com o passar dos anos, a expansão do comércio internacional intensificou o transporte de moedas, gerando desafios logísticos e de segurança devido às excesso de ouro e prata envolvidas, bem como ao risco de ataques de saqueadores e à falta de infraestrutura nas estradas (Lopes e Rossetti, 2005). O transporte de milhares de moedas representava um risco para a riqueza de comerciantes e governos importantes. Além disso, havia o problema da fraude, por pesagem imprecisa e a falsificação da pureza dos metais, problema que não pôde ser resolvido por completo pela estatização monetária. Embora os metais preciosos não sejam amplamente utilizados como meio de troca no mundo contemporâneo, eles continuam a ser empregados como reserva de valor (Soto, 2012), especialmente em tempos de crises financeiras, devido à sua oferta limitada.

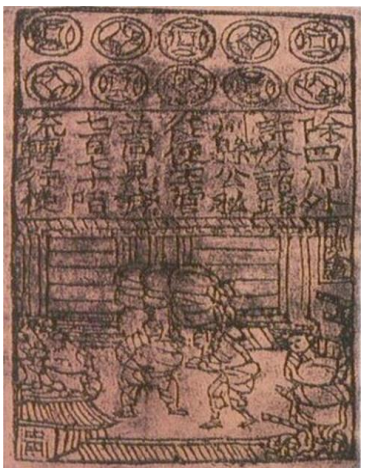
2.2 A MOEDA PAPEL

O papel-moeda refere-se a notas de dinheiro feitas de papel, geralmente emitidas por uma autoridade monetária, como um governo central ou

uma instituição bancária autorizada pelo estado (Lopes e Rossetti, 2005). Essas notas são usadas como meio de troca em transações comerciais e podem ser consideradas uma forma de dinheiro fiduciário, o que significa que seu valor não necessariamente está intrinsicamente ligado a um bem físico, mas sim à confiança e aceitação da sociedade. Entretanto, no início do desenvolvimento das primeiras moedas, sua conversibilidade era fundamental para a sua confiança. Portanto, o surgimento do papel-moeda é geralmente motivado pela necessidade de simplificar as transações comerciais, controlar a liquidez da economia e garantir a segurança no armazenamento de valores.

Os registros históricos indicam que o papel-moeda foi concebido na China durante a Dinastia Tang (618-907), com seu aprimoramento notável a partir dos anos 1.000, durante a Dinastia Song (Ibrachina, 2023). Denominado como "Jiaozi", essa inovação tinha o propósito de funcionar como uma nota promissória, representando uma garantia de valor metálico respaldada pelo governo, e era utilizada para realizar transações comerciais no cotidiano da população da província de Sichuan (Ibrachina, 2023). Essa medida visava reduzir a necessidade de lidar com grandes quantidades de moedas de ferro, ao mesmo tempo que evitava a saída de divisas metálicas para outros países. A Figura 2 ilustra um exemplar de uma cédula Jiaozi, confeccionada a partir de cascas de amoreira.

Figura 2 – Primeira papel-moeda



Fonte: BBC, 2017.[3]

[3] Disponível em: https://www.bbc.com/portuguese/geral-64260363. Acesso em 20, nov. 2023.

A introdução gradual da confecção de papel-moeda na Europa ocorreu tardiamente e foi implementada pelos principais bancos dos países. O Banco de Estocolmo, na Suécia, destacou-se como pioneiro no continente, realizando as primeiras emissões em 1661, seguido pelo Banco da Inglaterra e pelo Banco da França até o ano de 1700 (Vieira, 2017). Dessa forma, o uso generalizado de papel-moeda no continente europeu foi notavelmente tardio em comparação com a China. No Brasil, a primeira moeda impressa ocorreu em 1810, emitida pelo Banco do Brasil, evidenciado na Figura 3

Figura 3 — Primeira papel-moeda brasileira

Fonte: Banco Central do Brasil, 2004.

A modernização do sistema monetário, com a adoção do papel-moeda, proporcionou maior comodidade e simplificação nas transações comerciais, bem como na preservação de patrimônios. A introdução de meios como cheques, carimbados pela autoridade custodiante, permitiu que o valor de grandes fortunas fosse representado de forma eficiente. Esses fatores são apontados como contribuições significativas para o contínuo desenvolvimento do mercado.

Entretanto, à medida que a quantidade de moedas de ouro e prata sob custódia das instituições financeiras aumentou, estas perceberam a oportunidade de conceder empréstimos e emitir novos certificados sem o devido lastro garantido. Essa prática, popularizada no sistema bancário, é conhecida como reserva fracionária (Orrel e Chlupatý, 2016). As motivações para adotar esse sistema incluem a crescente demanda da sociedade por moeda, financiamento de guerras, desenvolvimento dos mecanismos de crédito e a implementação de políticas econômicas e sociais (Reverter, 2020). Esse

mecanismo torna-se viável, pois, em condições normais do sistema financeiro, os depositantes não solicitam a liquidação dos cheques simultaneamente, eliminando assim a necessidade de a instituição financeira manter toda a riqueza em estoque.

2.3 A MOEDA DIGITAL

O advento do dinheiro digitalizado representou uma transformação fundamental na história da economia e das finanças. A partir da década de 1990, a internet abriu as portas para o comércio eletrônico e a expansão dos serviços bancários online, permitindo que as pessoas gerenciassem suas finanças a partir de seus computadores pessoais (Lynch e Lundquist, 1996). No entanto, a mais notável popularização de uso se deu por meio de aplicativos bancários em smartphones, permitindo a realização de pagamentos, transferências e até mesmo investir em ativos financeiros de forma instantânea (Abdalla, 2017). Portanto, há um ganho de eficiência e produtividade nas negociações, pois se torna possível realizar transações à distância com maior rapidez, possibilitando o surgimento de diversos mercados.

Uma moeda digital pode ser definida como uma ferramenta monetária armazenada, manuseada e negociada por meio de arquivos digitais (Sabry, 2021). Nesse sentido, uma unidade monetária real deve equivaler em uma unidade virtual, expressa na plataforma bancária que o usuário utiliza. As instituições bancárias são, responsáveis pela segurança, custódia do patrimônio, e a compensação dos fundos no momento da negociação (Cardoso, 2018). Por se tratar de uma adaptação do sistema fiduciário às evoluções tecnológicas, ainda se faz presente o mecanismo de reserva fracionária, portanto, a moeda digital também sofre os efeitos da multiplicação monetária.

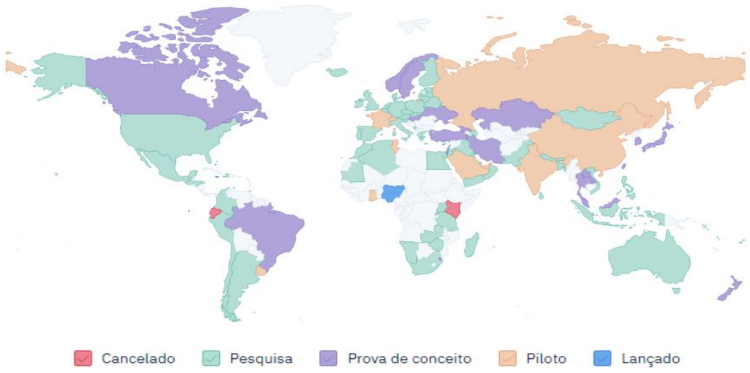
A popularização da moeda digital em pagamentos eletrônicos desmotiva o uso de dinheiro físico, principalmente em países desenvolvidos. Mais de 97% de toda a circulação monetária em dólar é feita digitalmente (Mookerjee, 2021). Na Suécia, a cédula não é mais utilizada como meio de troca, condição que torna o país completamente dependente da moeda digital (Fourtané, 2023). Outros países estão próximos de se tornar completamente livre de papel-moeda, tais como Finlândia, China, Coreia do Sul, Reino Unido e

Austrália (Corepay, 2021). De modo geral, os bancos privados e instituições de pagamento dominaram completamente o processo de transformação digital.

De modo a obter maior controle monetário, os principais bancos centrais mundiais estão desenvolvendo um novo modelo de dinheiro digital. Denominadas de *Central Bank Digital Currency* (*CBDC*), a autoridade monetária de cada país poderá centralizar os saldos patrimoniais e transações virtuais em seu próprio banco de dados. Portanto, a necessidade de uma instituição financeira privada validando as negociações entre os indivíduos pode ser dispensada (Ward e Rochemont, 2019). Ou seja, os estados buscam obter um maior nível de controle da economia por meio do processo da digitalização financeira em curso.

O Brasil é um dos países mais avançados no desenvolvimento de sua própria *CBDC*. Denominada de DREX, sua paridade será equivalente ao dinheiro físico ou digital, e deverá ser disponibilizado para o público em 2024 (BCB, 2023). Inicialmente, será necessário a utilização de aplicativos bancários privados, estes responsáveis por conectar os usuários com a rede principal do Banco Central do Brasil (BCB). Com isso, a promessa é utilizar contratos inteligente customizáveis, no qual as partes interessadas podem definir as condições de efetivação da transação, prometendo mais eficiência e segurança para os usuários (BCB, 2023). A Figura 4 mostra como as *CBDCs* está sendo implementadas no mundo todo, com informações atualizadas até outubro de 2023.

Figura 4 — Processo de implementação de CBDC em outubro 2023



Fonte: *CBDC Tracker*, 2023.[4] Adaptado pelo autor.

[4] Disponível em: https://cbdctracker.org/. Acesso em 15, out. 2023.

Há pelo menos dois países onde o plano de implantação foi cancelado, o Quênia e o Equador. Países como Estados Unidos, Chile, Argentina, Austrália e diversos países da União Europeia estão em fases de pesquisas iniciais. Canadá, Brasil e Japão estão em níveis avançados, com publicações na mídia acerca do funcionamento completo. Alguns países, incluindo Rússia, China, Índia, Arábia Saudita, França e Uruguai, possuem testes avançados sendo realizados em ambientes controlados. Por fim, apenas três países implementaram a *CBDC*, sendo eles Nigéria, Bahamas e Jamaica (*CBDC Tracker*, 2023).

Na medida que a discussão se expande no mundo, diversas críticas podem ser levantadas contra a introdução de uma moeda digital completamente centralizada por um banco central. Por exemplo, em caso de implementação da *CBDC* norte-americana, a China irá utilizar como meio de troca em suas negociações internacionais em dólar? A resposta parece óbvia, pois, não seria de interesse chinês que suas movimentações seja completamente rastreáveis em tempo real. Nessa mesma ótica, os principais oligarcas russos teriam interesse em ter sua privacidade patrimonial comprometida pelo banco central norte-americano? Caso seja uma figura politicamente exposta e ligada ao governo russo, certamente a resposta é não.

O Banco Central da Nigéria está enfrentando dificuldades no processo de implementação da sua *CBDC*. A introdução do eNaira, a moeda digital da Nigéria, teve como objetivo promover sua adoção entre os cidadãos, oferecendo incentivos como a fácil integração com contas bancárias existentes, um aplicativo para dispositivos móveis e um desconto de 5% em corridas de táxi (Packer, 2023). No entanto, mesmo com essas ofertas, os incentivos iniciais não foram suficientes para incentivar a adesão à moeda digital.

Em resposta, o governo nigeriano implementou restrições severas em dezembro, limitando os saques em dinheiro a 100.000,00 nairas ($225) por semana para indivíduos e 500.000,00 nairas ($1123) para empresas (Bludnik, 2023). Essas ações não foram bem recebidas pela população, e protestos surgiram na primavera de 2023, à medida que os cidadãos exigiam a reintrodução do dinheiro em papel. Os protestos incluíram ataques a caixas eletrônicos de bancos e bloqueios de ruas, com alguns manifestantes adotando

táticas violentas (*The Guardian*, 2023). A experiência nigeriana revela que o lançamento de uma *CBDC* pode enfrentar resistência significativa se for realizada forçadamente.

Em primeiro lugar, é crucial compreender as principais motivações apresentadas pelos governantes para a implementação de uma *Central Bank Digital Currency*. Segundo o *World Economic Forum* (*WEF*), os benefícios principais incluem: redução dos custos e do tempo de transação transfronteiriça, uma vez que a cobrança média atual é de 6,25%, com uma latência de até cinco dias úteis; aplicação eficiente de políticas públicas de assistência, como programas de renda básica; promoção da inclusão financeira, fator que contribui com a redução da pobreza e criação de empregos; e a capacidade de realizar um rastreamento completo das transações para combater a lavagem de dinheiro (Waliczek, 2023).

Diante dos benefícios mencionados, é possível realizar algumas reflexões. No que diz respeito à redução de custos e tempo de transações transfronteiriças, essa modalidade pode ser uma alternativa valiosa entre nações. No entanto, essa justificativa pode não ser uma novidade em território nacional para a realização de micropagamentos domésticos. Diversas instituições bancárias e de pagamentos já oferecem modalidades instantâneas e sem custo para transações nacionais nos principais países. Ou seja, a adoção de uma *Central Bank Digital Currency* como forma de pagamento nacional pode não ser plenamente justificada com base nesse argumento específico.

Em relação à aplicação de políticas de assistência, o argumento apresentado destaca a maior eficiência na entrega, especialmente para políticas emergenciais. No contexto brasileiro, esse ponto pode ser observado no caso do auxílio emergencial, um programa de renda básica criado para lidar com as problemáticas decorrentes da crise econômica e sanitária da COVID-19. O governo federal justificou a priorização do pagamento com base no número de identificação do Número de Identificação Social (NIS) (Cavallini, 2021). Para ilustrar, indivíduos com o final do NIS 1 receberam o auxílio em uma data específica, enquanto aqueles com NIS terminando em 2 receberam no dia seguinte, e assim por diante. Em resumo, o governo federal não demonstrou interesse em disponibilizar os recursos de forma imediata, optando por uma

entrega padronizada e sem atrasos por parte do sistema bancário. Embora possa haver dificuldades nesse sentido em países com sistemas bancários menos desenvolvidos, a realidade no Brasil e em outras principais nações do mundo não parece corroborar essa justificativa.

No que diz respeito à inclusão financeira, um fator de grande ênfase para sociedades com menos acesso ao sistema financeiro, é possível analisar o caso mencionado anteriormente sobre o experimento nigeriano com a adoção do eNara. Os resultados desse experimento não demonstraram ser inclusivos e benéficos para a população, pelo menos não da forma como foram implementados. Isso sugere que o argumento de inclusão financeira não é universalmente aplicável. Além disso, é importante observar que projetos de *Central Bank Digital Currency* estão sendo desenvolvidos em países tecnologicamente e financeiramente desenvolvidos. Sendo assim, não há uma evidente razão ou benefício esperado da *CBDC* em termos de inclusão financeira, uma vez que essa problemática já foi amplamente superada nessas nações.

A justificativa de rastreamento completo das transações, com a alegação de melhor prevenção à lavagem de dinheiro, é um fator que pode ser válido. De acordo com o relatório do *World Economic Forum*, as *Central Bank Digital Currencies* permitiriam a criação de registros digitais, facilitando assim a interrupção da lavagem de dinheiro e dos fluxos de dinheiro usados para financiar o terrorismo (Cavallini, 2021). No entanto, é importante destacar que a rastreabilidade adicional proporcionada pelas *CBDCs* pode afastar esse tipo de transação dos sistemas bancários formais, levando criminosos a procurar outras maneiras de contornar os regulamentos. Se isso ocorrer, a novidade pode tornar-se ligeiramente ineficiente e apenas suficientemente invasiva para a privacidade de cidadãos não criminosos.

Nos países onde os direitos à privacidade e à liberdade são consagrados em termos constitucionais, a introdução de uma *Central Bank Digital Currency* pode oferecer algum nível de benefício, embora possa implicar em uma perda substancial de liberdade, como o *WEF* busca justificar. No entanto, essa escolha pode ser prejudicial para a população em países com históricos de menos liberdade individual. Estados como o Brasil, Camboja,

Tailândia, Irã, Venezuela e China atualmente apresentam níveis relativamente baixos em termos de liberdade pessoal (Dupuis, 2021). Como destacado por Rothbard (2013), o poder que a moeda exerce na economia é significativo, sendo ela o elemento vital para o funcionamento de uma economia. Nessa lógica, a implementação de uma *CBDC* em países com históricos de menos liberdade individual pode aumentar o risco de aplicação de políticas tirânicas para cessar as liberdades individuais. Algumas possibilidades de controles podem incluir limites de transações, data de expiração de uso da CBDC, quotas e tarifas para determinados produtos, situações que podem acarretar um sistema análogo de crédito social.

Em síntese, a discussão sobre a implementação da *Central Bank Digital Currency* revela uma série de considerações complexas. Embora os benefícios apontados, como a redução de custos em transações transfronteiriças e a eficiência na aplicação de políticas de assistência, possam ser atrativos em cenários específicos, suas aplicabilidades e reais vantagens são questionáveis. Como mencionado por Rothbard (2013), a moeda, para desempenhar efetivamente sua função, deve ser selecionada pelos indivíduos no livre mercado e não determinada por lei. Em conclusão, para evitar graves problemáticas sociais semelhantes ao caso nigeriano, é crucial que o dinheiro seja um reflexo das demandas sociais e não exclusivamente uma imposição das autoridades.

3 O SISTEMA FIDUCIÁRIO

O termo "fiduciário" está relacionado com a confiança, o que significa que não tem algo como ouro ou outra garantia para sustentá-lo. É emitido apenas por governos e bancos centrais e é o único meio de pagamento aceito para pagar impostos e taxas, isso porque a lei obriga seu uso (Hayek, 2011). Essa categoria monetária pode estar na forma de notas de papel ou apenas em registros digitais, assim como as moedas representadas em contas bancárias e *CBDCs*.

É importante notar que a moeda fiduciária pode ser produzida de acordo com as necessidades da autoridade monetária, o que lhe confere a flexibilidade de ajustar a quantidade em circulação. As motivações para emissão são análogas às práticas de reserva fracionária no padrão-ouro citadas anteriormente, tais como fatores de demanda por moeda, investimento em defesa nacional, expansão no sistema de crédito e a implementação de programas sociais (Reverter, 2020). Com isso, há um forte estímulo para que políticos utilizem o poder de controle monetário para autofinanciamento de políticas públicas populistas, com o intuito de obter maior popularidade e permanência no poder.

Por ser uma modalidade regulada pela autoridade monetária, a moeda fiduciária é geralmente considerada segura pelos usuários, com menores riscos de fraudes. Com isso, além de fatores legais, ela é amplamente aceita tanto no comércio doméstico quanto nas transações internacionais, tornando-se um meio de troca amplamente adotado. Todavia, diversas são as críticas atreladas ao sistema *fiat*, no qual diversos casos serão evidenciados ao longo do capítulo.

Historicamente, um importante passo para o desenvolvimento do sistema fiduciário foi o surgimento do Acordo de Bretton Woods em julho de 1944. Este evento foi uma resposta à crise econômica global resultante da Grande Depressão de 1929 e da desintegração do sistema financeiro internacional (Barreto, 2009). Na época, as principais potências mundiais se viram confrontadas com a recessão, escassez de crédito, produção em queda e reservas cambiais em perigo. Sob a ameaça do protecionismo econômico e do nacionalismo, 44 países, incluindo o Brasil, se reuniram na cidade de Bretton Woods, nos Estados Unidos, para a Conferência Monetária e Financeira das

Nações Unidas. O objetivo primordial da conferência era redefinir a arquitetura financeira global, estabelecendo um sistema de regras que regulasse a política econômica internacional e promovesse a estabilidade monetária (Barreto, 2009).

O acordo resultante de Bretton Woods determinou que cada nação manteria a taxa de câmbio de sua moeda vinculada ao dólar. Por sua vez, o dólar dos Estados Unidos seria ancorado ao valor do ouro em uma base fixada (Bagus, 2011). Além disso, foram criadas instituições multilaterais, como o Banco Mundial e o Fundo Monetário Internacional (FMI), para monitorar o novo sistema financeiro e garantir a liquidez da economia global.

Um dos episódios que deu início ao processo de tornar a moeda fiduciária foi o processo de criminalização do uso do ouro como moeda. Um confisco do ouro nos Estados Unidos, ocorrido em 1933, foi uma medida controversa adotada pelo governo federal sob o pretexto de combater os efeitos da Grande Depressão. Sob a Lei de Emergência do Sistema Bancário de 1933 e emendas à Lei do Comércio com o Inimigo de 1917, o presidente foi dado o poder de confiscar o ouro das pessoas, forçando-as a entregar seu ouro em troca de papel-moeda (Woods, 2023). Embora tenha sido posteriormente revertido, esse episódio serve como um exemplo de como as interpretações e usurpações do governo podem distorcer a aplicação efetiva dos princípios constitucionais.

Anos depois, durante a década de 1970, os Estados Unidos enfrentaram um cenário de recessão decorrente de decisões de controle de capitais e taxação. Para abordar essa crise, o presidente do *Federal Reserve (FED)* implementou várias políticas monetárias expansionistas, incluindo significativas reduções nas taxas de juros e expansões substanciais na base monetária, um período conhecido como os "choques da era Nixon" (Beltrão e Geller, 2023). Consequentemente, ao longo do tempo, houve uma redução gradual do lastro do dólar com o ouro, o que efetivamente distorceu a ideia original do papel-moeda respaldado pelo sistema de padrão-ouro como guardião de valor.

Diante desse cenário, o conceito do padrão-ouro na realidade não era de forma alguma verificável. Com isso, um ponto histórico crucial aconteceu em 15 de agosto de 1971, quando o Presidente dos Estados Unidos, Richard Nixon, emitiu um decreto que significou o fim definitivo da ligação do dólar americano

ao ouro (Lopes e Rossetti, 2005). Esse evento marcou a transição do sistema baseado em lastro para o início de uma era em que a moeda depende inteiramente da confiança no sistema bancário, tornando-se completamente fiduciária.

Para Rothbard (2013), as autoridades estatais são incapazes de definir um bem para a função de meio de troca sem que esse bem tenha sido utilizado previamente pelos indivíduos para essa finalidade, pois o dinheiro emerge do livre mercado. Portanto, a centralização coercitiva da moeda seria uma distorção natural do que deveria ser o dinheiro: uma ferramenta livre, definida e valorada pelos indivíduos de forma descentralizada.

Caso a autoridade máxima seja ineficiente ou irresponsável na condução das políticas monetárias, as consequências são suportadas por toda a sociedade. Ao longo da história humana houve diversas catástrofes monetárias resultantes de expansões descontroladas da oferta de dinheiro, o que desencadeou grandes crises inflacionárias. A razão é que a emissão desordenada de moeda retira a riqueza dos indivíduos produtivos e a transfere para os controladores da moeda (Ammous, 2018). A Hungria, em 1946, enfrentou uma inflação diária de, aproximadamente, 207%, o Zimbábue registrou 98% em 2008, e a República Federativa da Iugoslávia experimentou uma inflação de 55% em 1994, eventos causados pela expansão descontrolada da oferta de dinheiro (Vasconcelos, 2021). Portanto, é evidente que em um sistema fiduciário, no qual o valor da moeda se baseia na confiança e na liquidez, a necessidade de previsibilidade e responsabilidade na condução da política monetária é extremamente necessária, embora nem sempre seja garantida.

De acordo com Hayek (2011), a inflação deve ser compreendida como a expansão da base monetária, e não pelos indicadores de variação de preço calculados pelas autoridades monetárias. Nessa perspectiva, a percepção de inflação pode ser ainda pior do que as informações divulgadas nas manchetes dos jornais. No Brasil, o Índice Nacional de Preços ao Consumidor Amplo (IPCA) é geralmente considerado o índice de inflação mais indicado. Conforme pode ser evidenciado na Tabela 1, a diferença é bastante considerável entre as variações anuais do IPCA e o crescimento anual da base monetária, representado pelo agregado M2, entre os anos de 2008 até 2022.

Tabela 1 — Variação percentual IPCA e M2 brasileiro

Ano	M2 (%)	IPCA (%)
2008	39,41	5,90
2009	9,12	4,63
2010	17,04	5,48
2011	18,88	6,74
2012	8,67	5,67
2013	10,74	6,26
2014	10,12	6,22
2015	6,75	8,53
2016	4,80	6,70
2017	5,54	3,43
2018	10,44	3,05
2019	8,70	3,69
2020	29,00	3,07
2021	8,05	7,37
2022	18,12	8,01
Média	**13,69**	**5,65**

Fonte: Elaboração própria. Dados disponíveis em: https://www3.bcb.gov.br/sgspub/.

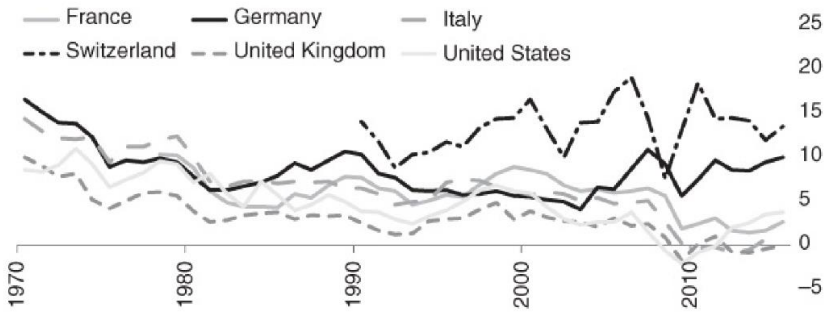
Conforme a Tabela 1, a média de crescimento anual da base monetária M2 foi de 13,69%, com dados de 2008 até 2022. No mesmo período, a média anual do IPCA foi de 5,65%. Esses dados podem indicar que o imposto inflacionário derivado da emissão monetária é quase três vezes maior que o índice comumente relacionado como inflação oficial.

A impressão desenfreada de moeda cria um processo de desvalorização perante outras moedas mais sólidas. Nesse contexto, o conceito da Lei de Gresham revela que os indivíduos, perante o processo inflacionário, buscarão alternativas de moedas mais sólidas (Rothbard, 2013). Nisso, ocorre um processo de desvalorização cambial, pois uma moeda melhor é menos requerida que a moeda pior. Ainda de acordo com Hayek (2011), o processo inflacionário cria um ambiente de estímulo ao endividamento populacional, contrariado a prática de poupar e investir. A inflação, portanto, reduz o padrão de vida no longo prazo, enquanto a ilusão monetária de dinheiro no presente gera uma sensação de prosperidade financeira falsa.

Essa situação também pode ser observada na redução sistemática do nível de poupança populacional, resultando em empobrecimento da população a longo prazo. Um indivíduo com baixa preferência temporal em relação às finanças é aquele que opta por utilizar a moeda como reserva de valor após satisfazer suas necessidades básicas, com a expectativa de ter um consumo maior no futuro, renunciando ao consumo no presente (Ammous, 2018). No

entanto, a expansão da base monetária resulta na transferência compulsória de riqueza da população para os bancos centrais, ocorrendo o chamado imposto inflacionário (Cysne, 1994). Como mostra a Figura 5, após o abandono do padrão ouro, os níveis de poupança das populações diminuíram ao longo do tempo.

Figura 5 — Níveis de poupança das principais economias 1970 – 2016



Fonte: Ammous, 2018. P. 91.

É intuitivo supor que, ao longo dos anos, com o desenvolvimento das economias, da tecnologia e o aumento da produtividade, a sociedade acumularia riqueza e aumentaria sua taxa de poupança, mas essa suposição não se concretiza. A Figura 5 revela uma queda sistemática nos níveis de poupança nas principais economias do mundo ao longo do tempo. O único país que manteve seu patamar elevado foi a Suíça. Esse movimento contrário pode ser explicado pelos substanciais reservas de ouro que a Suíça deteve até o ano de 1990, além do alto nível de segurança bancária oferecido pelo país (Ammous, 2018). Em suma, o argumento de Hayek de que uma economia expansionista desencoraja a poupança e estimula o consumo no presente se mostra verdadeira.

4 O BITCOIN

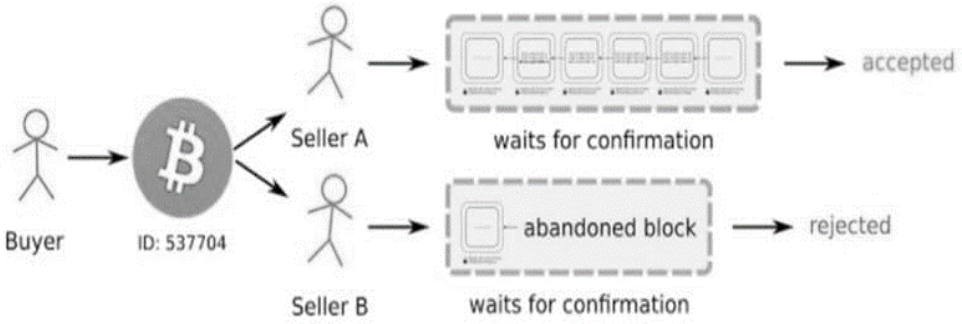
Como uma alternativa ao sistema financeiro centralizado, um usuário de um fórum virtual com o pseudônimo de Satoshi Nakamoto publicou em outubro de 2008 um artigo apresentando um projeto de uma alternativa de moeda virtual, denominada Bitcoin. Trata-se de um de projeto em código aberto, seu design é público, e ninguém possui o controle da rede (Nakamoto, 2008). Por ser uma tecnologia descentralizada, é dispensada a necessidade de instituições ou banco centrais. O gerenciamento das transações e emissões de novas unidades são realizadas coletivamente pela rede, denominada posteriormente de *blockchain*, utilizando mecanismos de criptografia avançada. O principal programador dessa ideia esteve ativo no progresso de desenvolvimento até o final de 2010. Desde então, muitas pessoas afirmam, ou afirmaram, ser “Satoshi”, mas até agora nenhum candidato conseguiu provar ser o criador.

Nesse mesmo ano, o mundo estava enfrentando as consequências da Crise do *Subprime*, caracterizada por uma forte crise de econômica que atingiu o setor bancário e imobiliário norte-americano em 2007, e suas consequências contaminaram a economia mundial durante anos. Como resposta à crise, uma das medidas do banco central norte-americano e de diversos governos de outros países foi de expandir consideravelmente a oferta monetária. As motivações era de estimular a economia e resgatar as instituições financeiras que estavam em processos de falência (Ulrich, 2014). Conforme evidenciado anteriormente, a emissão monetária exacerbada geralmente provoca graves consequências para a economia, desde perda de poder de compra e choques de demanda, fatores esses que tornam a sociedade mais pobre no longo prazo.

Quando o primeiro bloco de Bitcoin foi gerado, conhecido como bloco gênesis, uma mensagem foi propositalmente adicionada por Satoshi Nakamoto: "*The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*" (*Bitcoin.Wiki*, 2010). Essa mensagem é uma referência ao título destacado na capa do jornal The Times, na edição de 3 de janeiro de 2009, que informava que o governo britânico estava prestes a realizar um segundo resgate para os bancos utilizando recursos públicos. Essa escolha simbólica reflete a visão de Nakamoto sobre a fragilidade e as falhas do sistema financeiro tradicional.

Na prática, o Bitcoin opera em blocos dentro de sua própria rede, denominada *blockchain*, que valida e registra cada transação de forma pública, possibilitando a verificabilidade pelos usuários (Ammous, 2018). Assim, cada uma dessas transações é autenticada e registrada semelhante a um livro-razão. Isso é feito para prevenir o problema do gasto duplo, garantindo que cada fração de Bitcoin possa ser gasto apenas uma vez na rede. A Figura 6 fornece uma representação visual desse sistema:

Figura 6 — Processo de confirmação de bloco na *blockchain*



Fonte: Coinsultra, 2017.[5]

Conforme ilustrado na Figura 6, se um comprador tentar efetuar o pagamento para dois vendedores simultaneamente, a *blockchain* conseguirá identificar ambas as tentativas e aceitar apenas a primeira transação solicitada. A maneira que as negociações são registradas como um livro-razão garantem a organicidade desse sistema (Ulrich, 2014). Em resumo, a *blockchain* resolve o problema do gasto duplo em transações online de forma descentralizada.

Para o registro das negociações, agentes denominados de mineradores e validadores trabalham em conjunto para verificar a autenticidade dos blocos. Esse processo é chamado de *proof-of-work* (prova-de-trabalho) e requer que cada minerador use seu computador e energia para resolver um quebra-cabeça matemático (Ammous, 2018). Quando finalizado, as transações são efetivadas, os mineradores são recompensados com novos Bitcoins minerados, além das taxas pagas pelos usuários (Ulrich, 2014). Em resumo, é um sistema triangular de trabalho e recompensa. Os usuários pagam aos

[5] Disponível em: https://coinsutra.com/wp-content/uploads/2017/06/Bitcoin-Confirmations-e1498718174774.jpg. Acesso em: 06 set. 2023.

mineradores, que realizam esforços computacionais, verificados pelos validadores, que autorizam a transação.

A produção de novos Bitcoins está predefinida no código-fonte da criptomoeda. No ano de 2009, a gratificação concedida por bloco minerado a era, em média, 50 unidades, sendo que em 2024, esse valor será reduzido para 3,125. Esse comportamento é um fenômeno conhecido como *halving*, que ocorre aproximadamente a cada 4 anos, diminuição pela metade da recompensa, limitado à 21 milhões (Ammous, 2018). Sob essa dinâmica, novos blocos continuarão a ser gerados em um comportamento logarítmico, cada vez menor, tendendo à quantidade limite. Assim, o mecanismo de halving confere ao Bitcoin uma característica deflacionária. A Tabela 2 apresenta a projeção de recompensas ao longo do tempo.

Tabela 2 — Quantidade de Bitcoins por bloco minerado

Período	2009	2012	2020	2024	2032	2036	2044	2048
Recompensa (BTC)	50,00	25,00	6,25	3,13	0,78	0,39	0,10	0,05
Quantidade Diária	7.200,00	3.600,00	900,00	450,00	112,50	56,25	14,06	7,03

Fonte: Elaborado pelo autor.

De acordo com a projeção da Tabela 2, a partir de 2024, a criação diária de unidades atingirá 450, totalizando aproximadamente 164.250 BTC anuais. Em 2032, esse valor no mesmo período será de cerca de 41.062 BTC, enquanto em 2044, a quantidade anual se aproximará de 5.131 BTC. Em resumo, o processo de halving revela-se uma característica fundamental que confere ao Bitcoin uma superioridade sobre o padrão monetário fiduciário, uma vez que o torna imune à emissão por autofinanciamento.

Se a adoção do Bitcoin como meio de troca se concretizar, aliada à sua natureza descentralizada, é possível considerar o BTC como uma moeda, seguindo a classificação monetária proposta por Mises (1953). Dentro desse cenário, sob a ótica da Lei de Gresham, o Bitcoin poderia se tornar objeto de preferência monetária entre os indivíduos, potencialmente desvalorizando a moeda fiduciária estatal. Essa perspectiva se alinha com a proposta de dinheiro privado de Hayek, embora diferindo na necessidade de bancos privados.

O Bitcoin apresenta várias características que ressoam com os princípios aristotélicos essenciais de uma moeda. Sua durabilidade é assegurada pela validação e autenticidade registradas na *blockchain*. Além disso, é altamente portátil, uma vez que todas as unidades são armazenadas em uma carteira privada, com acesso garantido por meio de palavras-chave, permitindo a gestão de fundos em qualquer dispositivo com conexão à internet. No entanto, a fungibilidade do Bitcoin pode ser afetada no futuro, uma vez que transações de origem ilícita podem ser rastreadas na *blockchain*, resultando em bloqueios ou menor aceitação no mercado (Boyapati, 2021). Por outro lado, o Bitcoin é altamente divisível, podendo ser fracionado em unidades tão pequenas quanto 0,00000001 BTC, conhecidas como Satoshi (Antonopoulos; Osuntokun e Pickhardt, 2022). Essas características tornam o Bitcoin uma moeda digital única e versátil.

Adicionalmente, o Bitcoin exibe três características distintivas que merecem destaque: verificabilidade, escassez, resistência à censura e histórico de uso (Boyapati, 2021). A verificabilidade é uma qualidade inerente da própria *blockchain*, onde todas as transações, origens, destinos e utilizações são registradas de forma pública e transparente, permitindo uma verificação completa por qualquer pessoa. A escassez é uma característica fundamental do Bitcoin, uma vez que seu código-fonte estabelece uma política monetária que limita a emissão ao longo do tempo, resultando em um suprimento finito. Além disso, o Bitcoin é resistente à censura devido à natureza descentralizada da *blockchain*, que opera sem controle central, garantindo um nível significativo de privacidade e liberdade. Por último, o impacto histórico do Bitcoin na humanidade continuará a ser avaliado à medida que o tempo passa, solidificando seu lugar na evolução das finanças e da tecnologia.

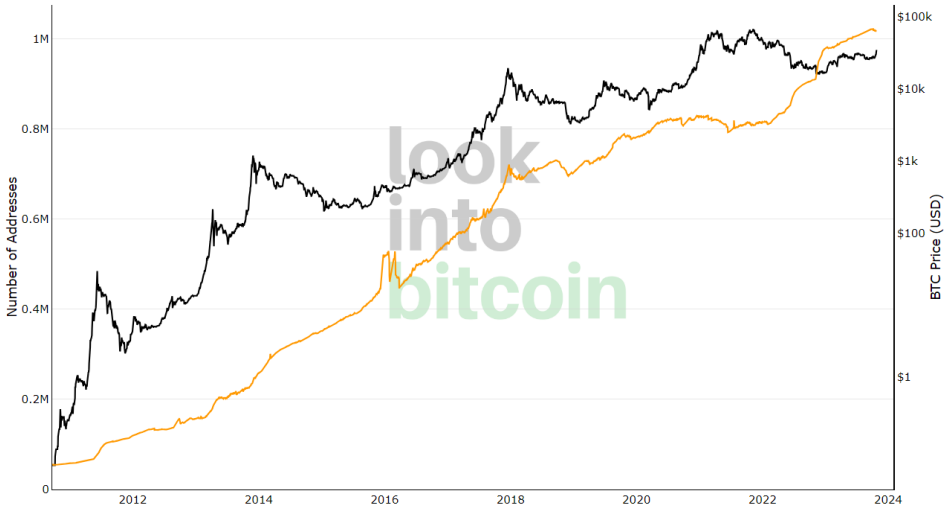
De modo comparativo, o Bitcoin apresenta notáveis distinções em relação às moedas fiduciárias, incluindo a *Central Bank Digital Currencies (CBDC)*. O Bitcoin é notável por sua descentralização, funcionalidade *peer-to-peer,* natureza de código aberto e processo de mineração, com uma oferta limitada de 21 milhões de moedas. Por outro lado, as moedas *fiats* estão sob o controle e emissão dos bancos centrais, necessitam de bancos intermediadores para realização de transações. O Bitcoin opera em *blockchain* pública e

verificável, com os usuários mantendo posse de suas próprias chaves privadas e desfrutando de anonimato. Em contraste, as *CBDCs* funcionarão em *blockchain* privada, sob o completo controle governamental. Assim, o Bitcoin rompe a ligação tradicional dos usuários com os bancos centrais, ao passo que as *CBDCs*, enquanto uma adaptação da moeda fiduciária, tende a ampliar o controle estatal da moeda.

3.1 A POPULARIZAÇÃO

A adoção do Bitcoin é bastante expressiva, e essa situação evidencia a perspectiva de valorização futura por parte dos usuários e empresas. O crescimento constante do preço do Bitcoin em relação ao dólar sugere um aumento na demanda por essa criptomoeda e seus fundamentos. Conforme Figura 7, o número de endereços de carteiras de criptomoedas com mais de 1,0 BTC em custódia cresce, assim como o preço expresso em dólar.

Figura 7 — Carteiras com mais de 1 BTC acumulado



Fonte: LookIntoBitcoin, 2023.[6]

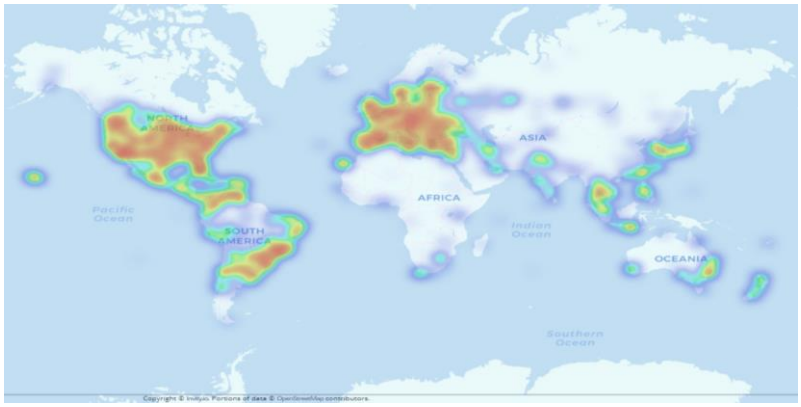
A tendência de aumento no número de endereços de carteiras com quantidades significativas de Bitcoin em custódia pode ser interpretada como um

[6] Disponível em: https://www.lookintobitcoin.com/charts/addresses-greater-than-1-btc/. Acesso em: 26, out. 2023.

sinal de confiança na criptomoeda por parte dos investidores e indivíduos que utilizam o Bitcoin como reserva de valor. A situação evidenciada na Figura 7 também ganha impulsos de caráter especulativos com processo de escassez ao longo do tempo, efeito ocasionado pelo *halving*. A teoria monetária exprime que, se uma boa moeda tem sua oferta reduzida, espera-se uma maior demanda, ocorrendo uma valorização o preço expressa em outra moeda (Ulrich, 2014). Portanto, caso a adoção continue crescente, os atuais acumuladores terão seu patrimônio valorizado no futuro.

Outro fator é a adoção em estabelecimentos comerciais ao redor do mundo. Aproximadamente 32.000 estabelecimentos, de diversos setores da economia, aceitam o Bitcoin como meio de pagamento (Coinmap, 2023). A Figura 8 mostra a distribuição geográfica desses estabelecimentos, destacando a crescente aceitação como uma forma de transacionar dinheiro em diversas regiões do globo, o que fortalece ainda mais sua posição como uma moeda digital de uso cotidiano.

Figura 8 — Mapa de calor da adoção do Bitcoin em 2023



Fonte: Coinmap, 2023.[7]

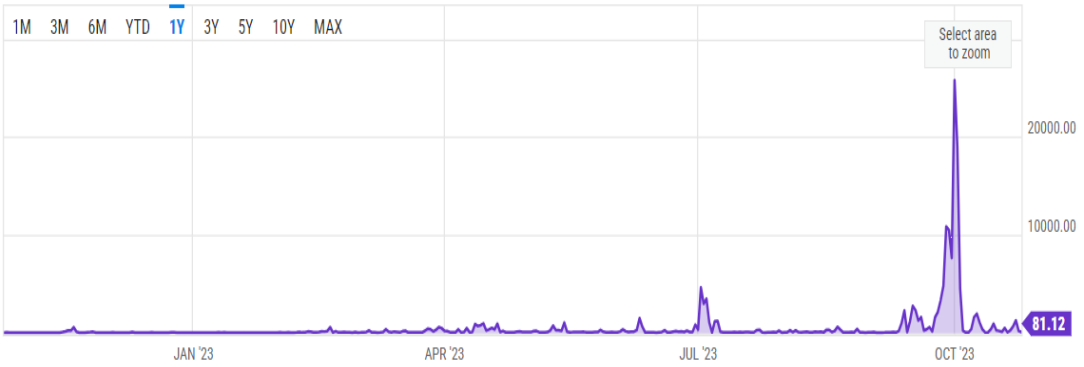
É visível na Figura 8 que, além do continente europeu e da América do Norte, os países emergentes da América Latina também possuem um espaço relevante na adoção do Bitcoin, especialmente a região sul e sudeste do Brasil. Esse fenômeno demonstra que o Bitcoin não está confinado a economias já estabelecidas, mas está desempenhando um papel crucial na inclusão financeira e no acesso a novas oportunidades de negócios em mercados emergentes.

[7] Disponível em: https://coinmap.org/view/#/world/56.21892319/-15.24902344/3. Acesso em: 03 set. 23.

3.2 O PROBLEMA DA ESCALABILIDADE

A popularização do Bitcoin demanda que a *blockchain* possua capacidade de operar em grande escala. O excesso de transações simultâneas de BTC cria uma fila de espera, e o usuário deve aguardar o descongestionamento ou pagar uma taxa maior (Antonopoulos; Osuntokun e Pickhardt, 2022). A depender do montante transacionado, a taxa da rede pode não compensar o uso constante do Bitcoin. Duas métricas podem ser utilizadas para compreender a situação de escalabilidade da rede: a latência para efetivar as transações e o custo por transação confirmada (Croman *et al.*, 2016). A respeito da latência, a Figura 9 evidencia a partir de outubro de 2022 diversos problemas de atrasos no tempo médio em confirmar as transações.

Figura 9 — Tempo médio de transação Bitcoin



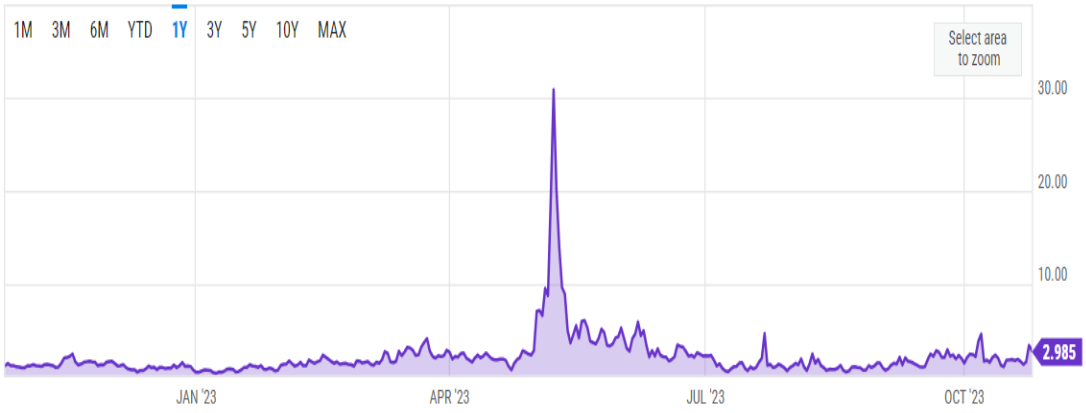
Fonte: Ychats, 2023.[8]

Conforme a Figura 9, o patamar registrado em outubro de 2023 ultrapassou 20.000 minutos, equivalente a aproximadamente 333 horas de tempo de espera. Se a rede permanecesse congestionada ao longo dos dias, seria necessário aguardar quase 14 dias para a conclusão da transação. Além disso, situações de estresse no tempo médio se mostram constantes ao longo dos meses, reforçando a necessidade premente de aprimoramentos na infraestrutura da *blockchain* para garantir uma experiência de transação mais

[8] Disponível em: https://ycharts.com/indicators/bitcoin_average_confirmation_time/chart/. Acesso em: 26 out. 23.

eficiente e acessível aos usuários. Observando o custo médio da taxa por transação, exposto na Figura 10, o cenário de instabilidade também é evidente.

Figura 10 — Custo médio de transação do Bitcoin (USD)



Fonte: Ychats, 2023.[9]

Diante do exposto, é notável perceber que em diversos momentos a taxa média por transação dispara, especialmente no período ocorrido entre abril e julho de 2023, alcançando uma média de USD 30,00. Esse problema também destaca a necessidade urgente de encontrar soluções que equilibrem a escalabilidade, custo e eficiência da *blockchain* para manter sua atratividade como um ativo e meio de transação confiável no mercado atual.

O Bitcoin possui um limite de tamanho de bloco de 1 megabyte, restringindo o número de transações que podem ser processadas em cada bloco. Como um novo bloco é gerado a cada dez minutos em média, isso implica que o Bitcoin pode processar aproximadamente apenas 7 transações por segundo (Ammous, 2018). Isso se traduz em um problema de escalabilidade significativa por limitar o potencial do Bitcoin como um sistema de pagamento global.

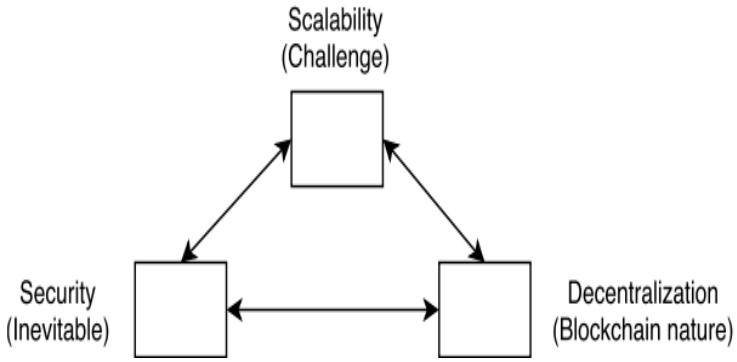
A atual literatura descreve que esse problema é derivado de uma limitação tecnológica no qual as *blockchains* só comportam simultaneamente dois dos três seguintes aspectos: descentralização, escalabilidade e segurança

[9] Disponível em: https://ycharts.com/indicators/bitcoin_average_transaction_fee. Acesso em: 26 out. 23.

(Hafid; Hafid e Samih, 2020). Trata-se do denominado “trilema da *blockchain*”, representada ilustrativamente na Figura 11.

.

Figura 11 — O trilema da blockchain



Fonte: Hafid; Hafid; Samih; 2020, p.2

Conforme demonstrado na Figura 11, segurança é inerente a *blockchain*, enquanto a descentralização é um pilar fundamental. No entanto, o trilema aponta a escalabilidade como um desafio latente. Analisando as características e a filosofia do Bitcoin, que possui ênfase na segurança e descentralização, se faz evidente a existência do “trilema da *blockchain*”, pois a escalabilidade é um problema constante.

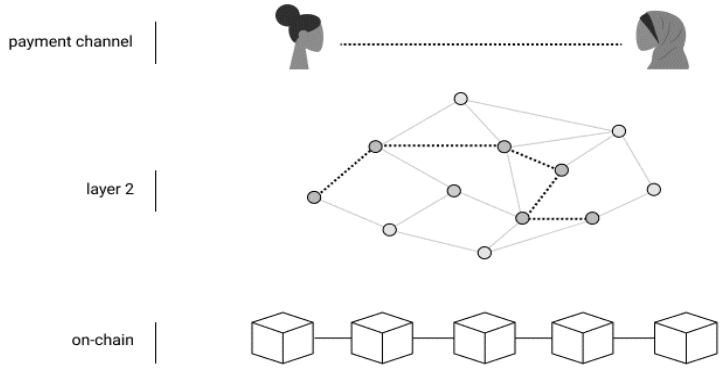
Para aprimorar a rede, modificações no protocolo são implementadas pelos desenvolvedores, que necessita da aprovação dos mineradores (Herrera e Pérez-Solà, 2016). Uma das propostas é aumentar o tamanho do bloco da *blockchain*, o que permitiria processar mais transações por segundo (Stasi *et al*., 2018). Entretanto, essa proposta não é vista com bons olhos por parte da comunidade envolvida, por se tratar de uma modificação brusca que pode impactar os outros aspectos que compõe o trilema da *blockchain*.

Uma alternativa viável é a instauração de uma rede secundária, uma solução de escalabilidade que opera em paralelo a *blockchain* primária do Bitcoin. (Antonopoulos; Osuntokun e Pickhardt, 2022). Existem várias implementações de segunda camada, sendo a *Lightning Network* uma das soluções mais populares para resolver os desafios de escalabilidade do Bitcoin (Reverter, 2020). Portanto, desenvolvedores e empresas estão trabalhando no desenvolvimento dessa rede alternativa, e diversos resultados positivos já podem ser evidenciados.

3.3 A LIGHTNING NETWORK

Para resolver a ineficiência da *blockchain* do Bitcoin em lidar com altos volumes de transações simultâneas, o protocolo *Lightning Network* foi desenvolvido por Joseph Poon e Thaddeus Dryja, publicado em janeiro de 2016. A LN é uma das soluções mais populares para resolver os desafios de escalabilidade do Bitcoin (Reverter, 2020). É definido como um protocolo em segunda camada que opera por meio de canais de pagamento, permitindo transações instantâneas em larga escala e com baixo custo operacional (Poon e Dryja, 2016). A Figura 12 ilustra essa questão.

Figura 12 — Canal de pagamento *Lightning Network*



Fonte: Opennode, 2021.[10]

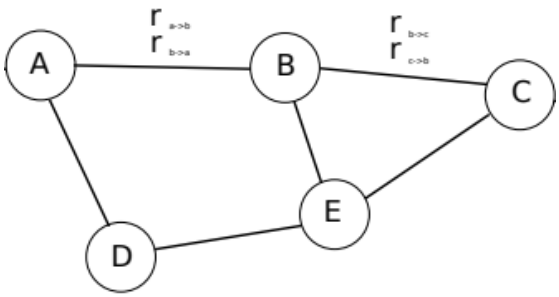
Com base no exposto, o indivíduo A (à esquerda) comunica a *blockchain* principal a abertura de um canal de pagamento em segunda camada com o indivíduo B (à direita), e então diversas transações podem ocorrer e serão registradas em um livro-razão. Portanto, cada nó é responsável por interagir com outros para transacionar BTC, enquanto os canais são essencialmente os caminhos que permitem as movimentações entre os nós da rede (Stasi *et al*., 2018). Com o encerramento do canal, o saldo final de todas as transações entre os dois indivíduos é registrado na *blockchain*.

Também é possível criar diversos canais conectados simultaneamente, formando uma grade rede de usuários interconectados. Em

[10] Disponível em: https://www.opennode.com/blog/bitcoin-transactions/. Acesso em 20 set. 2023.

outras palavras, os usuários intermediários são geralmente denominados de *hubs* (nós intermediários), e eles mantêm conectividade com vários usuários simultaneamente, recebendo pequenas taxas de roteamento como incentivo por seus serviços (Stasi *et al*., 2018). Os nós de maior conectividade são gerenciados principalmente por servidores empresariais. Esse serviço desempenha um papel crucial na descoberta de rotas para as transações, permitindo encaminhar fundos entre destinatários não conectados previamente. Essa situação pode ser melhor compreendida observando a Figura 13 abaixo.

Figura 13 — Canais de pagamento



Fonte: Stati *et al*., 2018. P. 5.

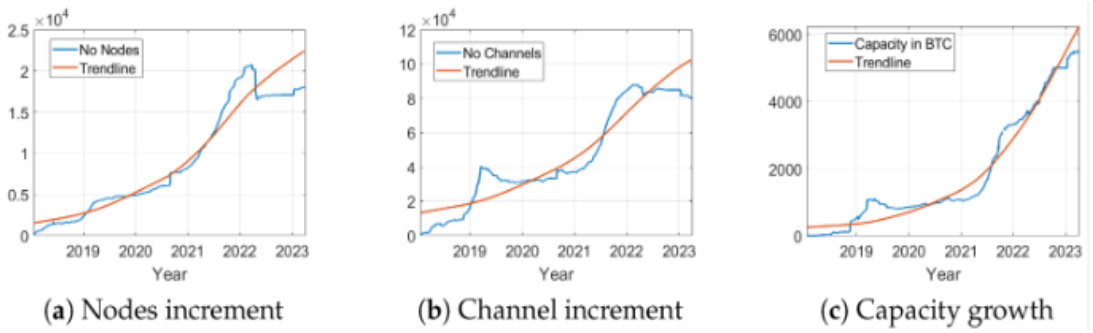
Diante da Figura 13, se o usuário A tem interesse em realizar um pagamento para o usuário C, não é necessário que eles criem um canal de pagamento exclusivo. Nesse caso, o usuário A pode utilizar sua conexão atual com o nó B, que completará a rota existente até o usuário C, mediante uma taxa de roteamento estipulada. Dependendo dos custos de transação e das preferências dos usuários, uma rota alternativa, que utilizaria os nós D e E, também pode ser escolhida.

Assim, a utilização da *Lightning Network* como uma alternativa de escalabilidade para facilitar micropagamentos em Bitcoin se destaca. A *blockchain* é conectada apenas na abertura e no fechamento de canais de pagamento em segunda camada (Poon e Dryja, 2016), possibilitando diversas transações eficientes enquanto aberto.

A adoção da *Lightning Network* como alternativa de escalabilidade para é crescente ao longo do tempo. Na medida que os usuários buscam acumular mais Bitcoins como reserva de valor, os indivíduos passam a negociar bens e serviços aceitando a criptomoeda como meio de troca. Conforme a Figura

14, existem notáveis crescimentos nas quantidades de nós (a), canais de pagamento (b) e capacidade em BTC (c).

Figura 14 — Crescimento da *Lightning network*



Fonte: Dasaklis e Malamas, 2023. P.4.

Com ênfase no item (c), o crescimento de liquidez na LN cresce fortemente, de aproximadamente 2.000 BTC em 2021 a quase 6.000 BTC em 2023. Essa situação representa um incremento de próximos de 200% de liquidez. Essa situação, aliada ao crescimento dos itens (a) e (b), representa um processo de adoção da LN como solução de escalabilidade.

O processo de adoção da *Lightning Network* está em expansão no Brasil, apresentando um potencial significativo em termos de alcance. Um notável experimento para popularizar esse ativo foi conduzido em uma escola pública de Jericoacoara, no Estado do Ceará, registrando um recorde mundial de transações na segunda camada. No curto período de 3 minutos e 33 segundos, foram realizadas 71 transações na região (Bertolucci, 2023). Esse caso simbólico, além de ter proporcionado uma recompensa em frações de Bitcoins para os alunos e residentes, pode atuar como uma estratégia de marketing, evidenciando que a *Lightning Network* pode viabilizar micropagamentos de maneira prática.

Para utilizar a *Lightning Network* de forma prática, os usuários geralmente optam por aplicativos de carteiras digitais. Entretanto, é necessário escolher entre uma carteira não custodiante, na qual o usuário mantém o controle direto de suas chaves privadas, e uma carteira custodiante, na qual um terceiro possui o controle da carteira. Cada abordagem possui vantagens e desvantagens, e a escolha adequada depende das necessidades individuais, nível de conforto e o conhecimento técnico.

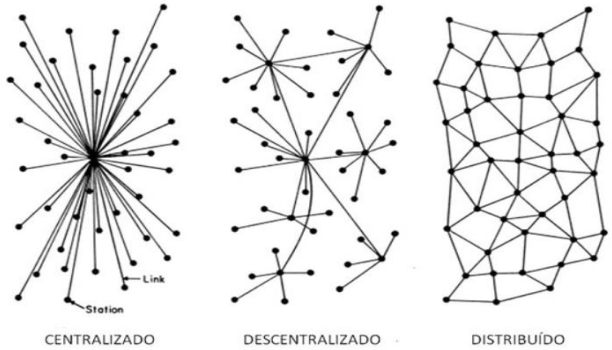
A carteira não custodiante é aquela na qual o usuário mantém o controle direto de suas chaves privadas. Uma carteira de controle próprio inclui todos os componentes essenciais, como gerenciamento de canais, sistema de roteamento de pagamento, funcionalidades que não dependem de terceiros (Antonopoulos, Osuntokun e Pickhardt, 2022). Portanto, uma carteira não custodiante possibilita ao usuário o máximo de controle sobre seus ativos, mas também implica uma maior responsabilidade na gestão do software e hardware.

Por outro lado, uma carteira custodiante possui um intermediário que atua como responsável no controle das chaves privadas dos usuários. Diversas empresas atuam nesse segmento, e as projeções indicam que o tamanho do mercado global de carteiras custodiantes deverá crescer para US$ 8,1 bilhões até 2025, a uma Taxa Composta de Crescimento Anual de 29,5% (*MarketAndMarket*, 2021). Esse tipo de carteira representa uma comodidade para o usuário, que não possui grandes preocupações em preservar as chaves privadas em segurança, visto que é ofertada pela empresa responsável.

Do que vem antes, é evidente o grau de importância que a descentralização tem para a existência das *blockchains*, pois se trata da gênese de sua existência. No Bitcoin, a proposta de Satoshi Nakamoto de substituir a necessidade de uma entidade central por uma solução ponta-a-ponta revolucionou a maneira como é vista a questão do dinheiro digital. Portanto, uma solução de escalabilidade requer a ausência de controladores, sejam eles privados ou entidades públicas, para que sua filosofia seja preservada. Nesse sentido, é necessário compreender a situação da *Lightning Network* no cumprimento deste aspecto, assim como a distribuição do mercado das carteiras com acesso à *Lightning Network*.

Quando se trata dos aspectos de rede, é imperativo compreender como deve ser configurada uma topologia de rede que opera sem controladores, a fim de avaliar se a *Lightning Network* preserva as características fundamentais do Bitcoin. Os sistemas de redes exibem uma diversidade de aspectos topológicos que podem ser identificados e analisados. Na Figura 15, três principais características de modelos são evidenciadas: centralizado, descentralizado e distribuído.

Figura 15 — Arquiteturas de rede

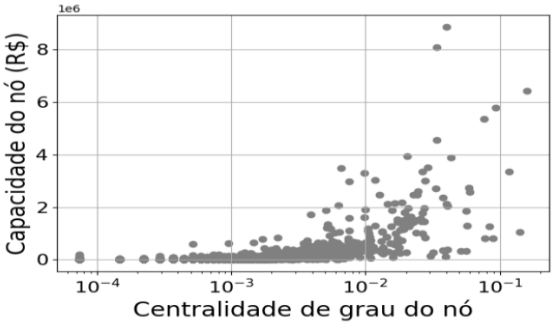


Fonte: adaptado de Paul Baran, 1962. P.4.

Diante da Figura 15, percebe-se que o conceito centralizado mostra em um controle completo absoluto por poucos. Para as redes descentralizadas e distribuídas, não há uma entidade com poder suficiente para controlar completamente a rede. É esperado, que a *Lightning Network* apresente um padrão gráfico semelhante aos modelos distribuído e descentralizado.

Um estudo conduzido por Camilo *et al*. (2022) se deu por uma investigação significativa no âmbito da *Lightning Network*, baseando-se em dados empíricos obtidos entre janeiro de 2020 e agosto de 2021, com o interesse de averiguar possíveis aspectos de centralização na *Lightning Network*. Os resultados deste estudo evidenciaram um absoluto grau de centralização de renda e conectividade na LN. Segundo os achados, apenas 0,38% dos nós concentraram surpreendentemente 50% de capacidade total da rede (Camilo *et al*., 2022). A visualização da Figura 16 exprime de forma gráfica essas informações: a relação entre o grau de centralidade dos nós e a capacidade de renda.

Figura 16 — Distribuição da capacidade de roteamento dos canais de rede

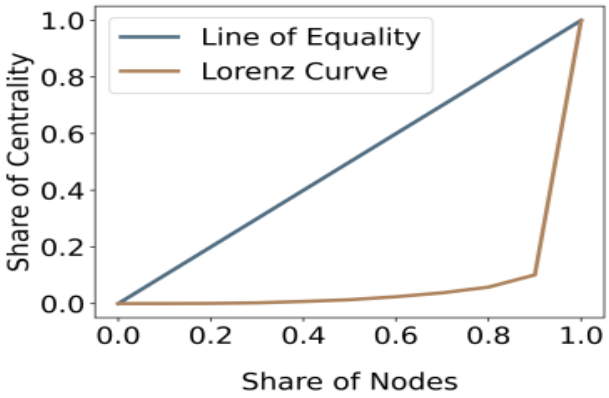


Fonte: Camilo *et al*., 2022. P. 6

Conforme a ilustração, existe uma forte tendência de correlação positiva entre o grau de centralidade de um nó e sua capacidade de roteamento de transações, resultando em maior receita para aqueles que a controla. Esse resultado pode ser fundamentado na perspectiva que, na medida que cresce os usuários na rede, estes irão preferir se conectar com nós de maior liquidez e conectividade, facilitando as operações de micropagamentos (Camilo *et al*., 2022). Com isso, a situação representa um estímulo para uma maior centralização da rede à medida que novos usuários utilizem a LN.

Um segundo estudo realizado por Zabka *et al*. (2022) também utilizou dados reais de anúncios e canais de pagamento da LN, porém com dados de 1º de abril de 2019 até 1º de janeiro de 2021. Diferente de Camilo *et al*. (2022), O modelo estatístico determinado pelos autores para entender a centralidade da rede foi o Coeficiente de Gini. Esse modelo é geralmente utilizado para medir o nível de desigualdade em uma determinada nação ou grupo social (Wolffenbüttel, 2004), mas sua capacidade também pode ser aplicada para identificar o grau de concentração na LN, evidenciado na Figura 17.

Figura 17 — Coeficiente de gini (*LN*)

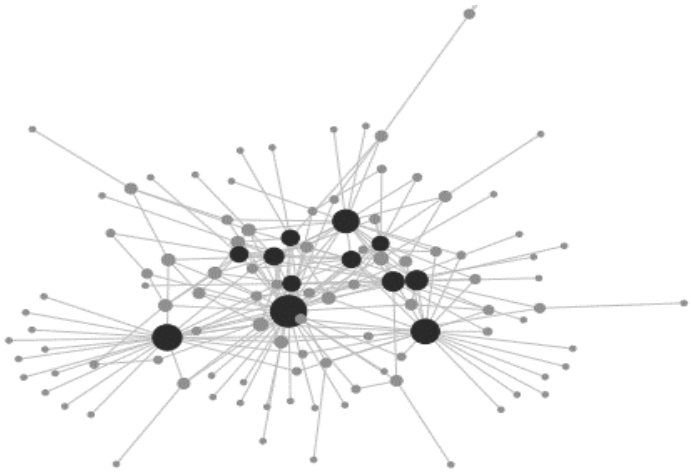


Fonte: Zabka *et al*., 2022. P.8

Os resultados revelam que aproximadamente 90% dos nós contribuem apenas com 10% da intermediação das transações. Isso implica que uma parcela significativamente pequena concentra quase completamente a capacidade de intermediação na *Lightning Network*. Essa constatação reforça a tese de uma forte presença de centralização na LN.

Um terceiro estudo, conduzido por Lin *et al*. (2020), apresentou resultados consistentes os dos autores anteriores. Esse estudo abrangeu um período de análise que se estendeu de 12 de janeiro de 2018 a 17 de julho de 2019, e uma das abordagens utilizadas foi o *core-periphery model* (modelo de núcleo-periferia), que permitiu uma visualização topológica da estrutura da rede, como ilustrado na Figura 18.

Figura 18 — Estrutura de divisão centro-periferia da LN

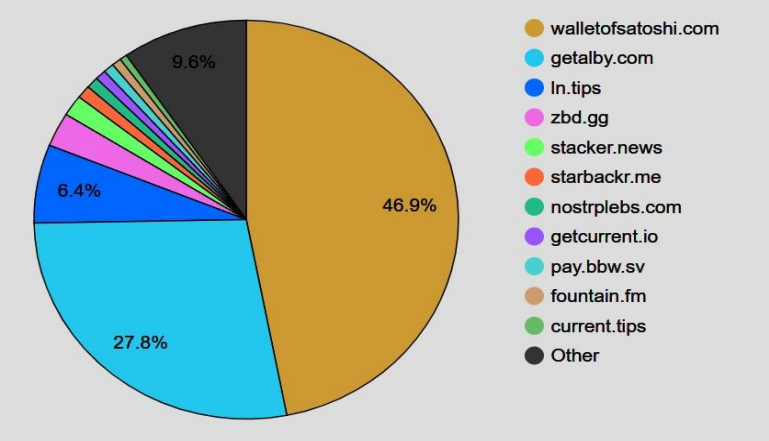


Fonte: Lin *et al*., 2020. P. 8

Os resultados do modelo de núcleo-periferia apresentam uma situação que se assemelha, em comparação com a Figura 15, a uma topologia próxima à centralizada. Os resultados estatísticos indicam que, em média, cerca de 10% dos nós controlam aproximadamente 80% da *Lightning Network* (Lin *et al*., 2020). Esse cenário centralizado, assim como verificado nos demais estudos, pode levantar questões sobre a ameaça da LN enquanto solução para o Bitcoin.

Quanto à maneira como os usuários acessam a rede, os dados indicam que a maioria deles recorre a carteiras custodiantes. A plataforma de rede social Nostr, reconhecida por sua operação anônima e descentralizada, está testemunhando um aumento significativo nas microtransações realizadas pelos usuários, denominadas "zaps". Cerca de 11.500 endereços de carteiras estão envolvidos nessas transações, sendo que 93% delas têm origem em carteiras custodiais (Zapalytics, 2023). Essa relação por empresa pode ser visualizada na Figura 19.

Figura 19 — Endereços LN por aplicativos no Nostr



Fonte: Zapalytics. Disponível em: https://zapalytics.com/. Acesso em 25 set. 2023.

A Figura 19 destaca que a Wallet of Satoshi, um aplicativo de carteira com acesso à LN, detém 47% de todos os nós conectados, enquanto a Alby, que oferta o mesmo serviço, representa quase 28%. Somados, aproximadamente 75% dos usuários dessa rede social utilizam apenas dois aplicativos de empresas custodiantes. Essa situação evidencia uma concentração crítica do mercado de carteira em torno de poucos players.

O advento do Bitcoin, por meio da tecnologia *blockchain*, trouxe consigo promessas de descentralização e segurança, representando um contraponto aos padrões do sistema financeiro. A *Lightning Network* é a principal candidata para resolver os problemas de escalabilidade e velocidade nas transações do BTC (Antonopoulos, Osuntokun e Pickhardt, 2022). No entanto, o cenário atual da literatura evidencia uma situação preocupante em relação à centralização da *Lightning Network*.

Conforme evidenciado, a *Lightning Network* funciona atualmente com *hubs* centralizados para realizar transações (Camilo *et al*., 2022) (Zabka *et al*., 2022) (Lin *et al*., 2020). Além disso, indícios mostram que grande parte dos usuários acessam a *Lightning Network* por carteiras custodiantes de apenas duas empresas privadas (Zapanalytics, 2023). Nesse sentido, se faz necessário elencar os principais riscos associados à filosofia do Bitcoin enquanto moeda digital descentralizada.

Quando um usuário deseja se conectar a um nó centralizado, este pode identificar o endereço de protocolo de rede (IP), situação que expõe a geolocalização aproximada (Antonopoulos, Osuntokun e Pickhardt, 2022).

Embora existam várias maneiras de camuflar o IP, tais como o uso de *Virtual Private Network* (*VPN*) e *The Union Router* (*TOR*), essas soluções são alheias ao funcionamento padrão da rede. Em um cenário de sanção econômica, por exemplo, no qual usuários de determinados países são impedidos utilizar *hubs* empresariais, a localização por IP pode privar o acesso do indivíduo, sendo necessário utilizar novas rotas de pagamento ou serviços de camuflagem de IP.

Acerca de aspectos de segurança, na medida que poucos *hubs* se concentram na rede, estes se tornam alvos de ataques cibernéticos. Ferramentas de agressão direcionada podem incluir ataques de negação de serviço (*DDoS*), que causam congestionamentos excessivos na rede, e ataque eclipse, situação já ocorrida que possibilitou roubo de fundos (Riard e Naumenko, 2020). Ainda que soluções e melhorias para pontuais ataques sejam aplicadas, os estímulos para os agentes maliciosos continuarem encontrando falhas é evidente, pois poucos *hubs* concentram grandes volumes de Bitcoins.

Outro aspecto de risco é a modificação de taxas de transações em seus canais centralizados (Poon e Dryja, 2016). Com isso, por qualquer motivo que seja, uma modificação tarifária pode ser implementada e prejudicar os usuários conectados no *hub*. Embora essa flexibilidade possa ser vista como uma estratégia de negócios legítima, e a solução seja se conectar em outro *hub*, eventuais problemas de congestionamento sistemático pode tornar cara toda a rede por algum tempo.

Acerca de aspectos regulatórios, os reguladores podem classificar as empresas que realizam gestão de *hubs* como prestadores de serviços financeiros, pois estes obtêm lucros por taxas de rede. Para que a empresa se regularize, modificações nas regras de consenso de conectividade podem ser aplicadas. Leis de investigações acerca de lavagem de dinheiro certamente irão exigir informações mais apuradas dos usuários da rede.

Com ênfase em carteiras custodiais, os usuários podem comprometer sua privacidade com as empresas responsáveis (Nair e Song, 2023). Informações como padrões de consumo, geolocalização e controle de fundos são armazenados e geridos por terceiros. Nesse cenário, não haveria diferenças perante instituições financeiras tradicionais.

Acerca de aspectos de segurança, diversos riscos significativos, como ataques hackers, também podem ser observados. Os criminosos geralmente exploram vulnerabilidades na infraestrutura de segurança dos servidores privados das empresas que custodiam as chaves privadas dos usuários (Hu *et al*., 2021). Com acesso as chaves privadas, é possível realizar saquear dos fundos de criptomoedas da carteira do cliente para a carteira do invasor. Além disso, outros dados pessoais, como endereços de e-mail e senhas, também são geralmente expostos. Esse tipo de ameaça destaca a importância de robustas medidas de segurança cibernética ao lidar com sistemas que envolvem transações financeiras e informações sensíveis.

Uma prática comum entre empresas de carteira custodial é a realização de movimentações de BTC entre seus clientes sem registros nas camadas primária ou secundária. Essas transações "off-chain" são comumente utilizadas por essas entidades (Bains *et al*., 2022). Essa abordagem permite que tais empresas operem sem a necessidade de manter reservas equivalentes aos saldos de seus usuários, abrindo espaço para o risco de "criação de Bitcoins" por meio de reserva fracionária. Um exemplo notável de uma situação semelhante ocorreu com a FTX, uma das maiores corretoras de criptomoedas, na qual esse tipo de fraude contábil comprometeu o patrimônio de milhares de clientes (Chohan, 2023).

Além disso, as modificações tarifárias e o bloqueio de saques são aspectos críticos que demandam atenção. No cenário atual, diversas empresas de carteiras e corretoras adotam a estratégia de oferecer taxas reduzidas para atrair clientes. No entanto, em situações de problemas técnicos, como no caso da FTX, políticas tarifárias e restrições de saques podem ser implementadas para evitar o colapso da empresa.

O cumprimento de obrigações legais já é uma exigência comum para esse tipo de carteira, incluindo a conformidade com regulamentações *Know Your Customer* (*KYC*), que demandam a coleta de informações pessoais e financeiras dos clientes (Malhotra *et al*., 2021). Na União Europeia, a aprovação da *Markets In Crypto-Assets Regulation* (*MiCAR*) estabelece a obrigatoriedade da coleta de dados de todos os usuários de carteiras de criptomoedas (*European Securities and Markets Authority*, 2023). Apesar das motivações dos usuários em busca de

privacidade patrimonial, as características essenciais do Bitcoin visam garantir isso, uma situação que pode não ser assegurada ao utilizar esse tipo de carteira.

3.4 OS CONTRATOS DE BITCOIN

Adicionalmente, merece destaque a modalidade de negociação de contratos de Bitcoins, comumente denominadas de “Bitcoins de papel”. Nessa prática, uma empresa ou instituição bancária declara a posse dos ativos e emite contratos digitais representativos. Esses contratos representam, na realidade, uma dívida ou uma promessa de que o papel ou contrato acompanhará o preço do Bitcoin. Ao longo de anos, instituições financeiras e bancos adotaram a prática de oferecer ativos digitais, como o Bitcoin, sob a forma de contratos, em detrimento da utilização do registro direto na *blockchain*.

A consequência direta é que os detentores desses contratos perdem a capacidade de efetivamente controlar e retirar os fundos para mantê-los em suas próprias carteiras de autocustódia, resultando na perda de propriedades intrínsecas que tornam o Bitcoin disruptivo ao sistema fiduciário. Com isso, é necessário confiança na empresa, que geralmente irá emitir relatórios de comprovações de fundos, que podem ser fraudados, assim como o caso da FTX. A negociação de contratos sem o devido lastro garantido distorce significativamente o preço de mercado, havendo expansão de oferta por meio da atividade de reservas fracionárias. Nesse sentido, ocorre essencialmente recriando o sistema fiduciário.

No Brasil, diversos bancos tradicionais e instituições de pagamento digital estão ofertando a compra e venda desses contratos. O Nubank, instituição de pagamento que conta com mais de 80 milhões de clientes, oferece a negociação em seu aplicativo para smartphones, com valores a partir de R$ 1,00 (Nubank, 2022). Segundo a instituição, a custódia é de responsabilidade compartilhada com a norte-americana *Paxos Trust Company*, empresa completamente regulamentada pelo *FED*, lhe garantindo maior confiança. Todavia, com mais de R$ 130 milhões em alocações em criptomoedas dos clientes, o Nubank afirma que os usuários não poderão realizar saques para carteira de autocustódia na *blockchain* (Honorato, 2023). Em outras palavras, a

compra de Bitcoin através dessa plataforma oferece apenas função especulativa na volatilidade do ativo.

A Méliuz S.A, empresa de tecnologia que possui uma base de clientes acima de 20 milhões, se destaca por oferecer ao cliente que realiza compras online cupons de descontos e o serviço de cashback, que retorna uma porcentagem do valor total de compras online. Em busca de se adequar ao mercado monetário de criptomoedas, a instituição implementou a função de compra, venda e cashback em Bitcoin (Méliuz, 2023). Todavia, assim como o Nubank, a Méliuz ainda não oferta a possibilidade de saques para carteira de autocustódia na *blockchain*, nem mesmo em segunda camada via *Lightning Network*.

Recentemente, o governo de Israel anunciou no dia 10 de outubro de 2023 o confisco de diversas criptomoedas, inclusive de Bitcoins, do grupo terrorista Hamas. Isso foi possível, pois as quantias eram armazenadas na corretora Binance, que colaborou com as autoridades israelenses (Marins, 2023). O Hamas não se preocupou em realizar a autocustódia, mesmo sendo um notável alvo de investigações por órgãos de espionagem, resultando em evidentes prejuízos financeiros. Caso os usuários busquem a negociação de Bitcoin por meio de plataformas digitais centralizadas, o controle monetário de grandes corporações e autoridades estatais poderá surtir efeito tão quanto o uso direto de uma *CBDC*. Apesar de os usuários convencionais não estarem envolvidos em atividades criminosas, é relevante destacar que em países autoritários, onde práticas de censura e perseguição política são recorrentes, instituições financeiras, incluindo corretoras e bancos, podem desempenhar um papel colaborador com o estado na restrição do acesso aos recursos patrimoniais dos clientes.

A rede social X, anteriormente conhecida como Twitter, está obtendo gradualmente licenças nos Estados Unidos para custódia, negociação e transferências de moedas digitais. Essa movimentação representa um passo significativo em direção a se tornar uma "plataforma completa", capaz de fornecer serviços de pagamento abrangendo tanto criptomoedas quanto moedas tradicionais. Apesar dos relatos iniciais indicarem que o serviço de pagamentos do X se concentrará em moedas fiduciárias, o CEO da empresa, Elon Musk,

instruiu a equipe de desenvolvedores a projetar o sistema de pagamento de modo a permitir a futura incorporação de criptomoedas, incluindo o Bitcoin (Mitchelhill, 2023). Se isso ocorrer, os usuários poderão possuir e negociar o ativo diretamente na plataforma X. Sendo uma das redes sociais mais amplamente utilizadas no mundo, caso os usuários não priorizem a autocustódia, o Bitcoin pode enfrentar mais um desafio de negociação centralizada.

É crucial destacar que as situações que envolvem contratos de Bitcoins e reservas fracionárias realizadas por intermediários não impactam as características intrínsecas do ativo, conforme programado em *blockchain*. Em outras palavras, a moeda permanece descentralizada e com escassez programada em seu código-fonte. No entanto, sua utilização de contratos ou promessas por meio de intermediários centralizados, além de resultar em distorção de preço, torna a moeda apenas mais uma ferramenta fiduciária de alta volatilidade.

5 A IMPORTÂNCIA DO BITCOIN NO MUNDO FIDUCIÁRIO

Desde que o Bitcoin obteve uma considerável popularização, diversos economistas, revistas renomadas e autoridades afirmaram que a moeda não teria forte relevância no sistema financeiro. Um curioso site chamado 99bitcoins reúne quantas vezes a moeda foi declarada pela mídia tradicional como “morta”. Atualmente, o Bitcoin 'morreu' 474 vezes, sendo o ano de 2017 o que teve o maior número de ocorrências dessas notícias, totalizando 124 (99bitcoin, 2023).

Em sentido similar, Larry Fink, *CEO* da *BlackRock*, a maior gestora de fundos do mundo, afirmou em entrevista em 2017 que o ativo seria apenas uma invenção para lavagem de dinheiro (Imbert, 2017). Entretanto, o gestor mudou sua perspectiva ao longo do tempo, afirmando que o Bitcoin é como um “ouro digital” (Malar, 2023). Recentemente, a *BlackRock* vem se movimentando para obter licença de negociação de seu próprio contrato de Bitcoin (Rubinstein, 2023).

Assim como a antiga perspectiva de Larry Fink, diversos reguladores estatais continuam a considerar o Bitcoin uma moeda associada a atividades criminosas. A China, por exemplo, proibiu tanto o uso quanto a mineração da criptomoeda, alegando "inutilidade" e envolvimentos em "crimes cibernéticos" (*CNN*, 2023). No entanto, de forma intrigante, a China permanece como um dos principais países em termos de mineração da moeda, contribuindo com aproximadamente 22,29% do poder computacional global (Kaloudis, 2022). Isso evidencia que os usuários e mineradores veem o Bitcoin como uma alternativa lucrativa, a ponto de desrespeitar a legislação vigente em seu país.

Diante dos diversos problemas associados ao sistema *fiat*, o uso do Bitcoin pode representar uma alternativa benéfica. A Nigéria, por exemplo, que registrou baixa adesão às *CBDCs*, é o segundo maior país em termos de uso de criptomoedas, sendo a Índia a primeira colocada e o Vietnã o terceiro (Jenkinson, 2023). Na Venezuela, o Bitcoin se tornou uma alternativa para muitos indivíduos em resposta aos altos índices de inflação (Martin, 2021). Da mesma forma, na Argentina, com uma inflação anual de aproximadamente 100%, a valorização do Bitcoin tem crescido significativamente devido à alta demanda (*Investing*, 2023). Nesse sentido, a existência de uma criptomoeda que está livre do controle

governamental se torna necessária, especialmente em países que enfrentam sérios problemas econômicos.

Recentemente, milhares de ucranianos fugiram para outros países, especialmente na Europa, em resposta à intervenção russa em seu território nacional em 2022. No entanto, os homens em idade militar foram impedidos de deixar o país, e seus bens foram bloqueados como represália (G1, 2022). Como resposta, muitos ucranianos recorreram ao Bitcoin como uma forma de contornar o controle de capitais do governo local em seu processo de fuga (Zanatta, 2022). Portugal, sendo um dos países da União Europeia que tem se tornado atrativo para os usuários de criptomoedas, tornou-se um dos destinos escolhidos pelos imigrantes (Pedro, 2022). Em resumo, o Bitcoin, com todas as suas características positivas já mencionadas, também se apresenta como uma alternativa para a preservação de capital por parte de indivíduos em países que enfrentam crises severas e controles estatais.

Situações de bloqueio de contas bancárias, controles de capitais, perseguições políticas e medidas autoritárias dos governos podem se intensificar com o uso da tecnologia. Como já mencionado, o desenvolvimento das *CBDCs* pode ser mais um fator que aumenta esses problemas, especialmente com a tendência de queda no uso de papel-moeda. Nesse processo, vários países da União Europeia vêm desencorajando o uso de dinheiro físico, e algumas empresas já não o aceitam como método de pagamento (Fourtané, 2023). Nesse sentido, em alguns anos, o uso das *CBDCs* será mais do que necessário, representando um forte risco à privacidade e à autonomia financeira dos cidadãos.

Diante das problemáticas da centralização monetária, surge a concepção de um livre mercado de moedas privadas como uma solução ao sistema fiduciário. De acordo com Hayek (2011), não há motivos para duvidar da capacidade de um sistema monetário privado, visto que assim foi o surgimento e o desenvolvimento das moedas anteriormente. É coeso imaginar que, devido aos mecanismos da Lei de Gresham, oferta, demanda e lucro, as empresas que produzirem uma moeda fraca para o mercado seriam aniquiladas financeiramente, sobrevivendo apenas as empresas comprometidas e eficientes na questão monetária. Portanto, considerando que uma das características da

moeda é a reserva de valor a longo prazo, é razoável que as entidades responsáveis por suas moedas privadas trabalhem para preservar seu valor, em vez de deteriorá-lo, estimulando níveis mais elevados de poupança e riqueza. Ou então, como no caso do Bitcoin, seu controle é descentralizado e livre do risco empresarial.

Nesse sentido, dois aspectos devem ser buscados para obter uma moeda robusta em uma economia descentralizada: a moeda definida como meio de troca pelo livre mercado e sua capacidade de resistir ao sistema monetário centralizado (Mises, 1953). Em última análise, a busca por uma moeda forte e estável requer não apenas uma abordagem descentralizada e orientada pelo mercado, mas também a vigilância constante para garantir que a preservação de valor a longo prazo seja uma prioridade, minimizando assim os impactos adversos sobre a sociedade.

O Bitcoin tem se mostrado como um forte candidato para auxiliar indivíduos que enfrentam problemas no âmbito monetário e estatal. Em outras palavras, ele se encaixa bem nas perspectivas de moeda privada propostas pelos economistas austríacos. Isso pode significar que, à medida que os países conduzem suas políticas monetárias de forma inadequada, haverá incentivo para que os indivíduos troquem sua moeda nacional pelo Bitcoin. Esse é o cenário na Nigéria, onde o Bitcoin negociado em corretoras locais estava, em média, 60% mais caro do que em corretoras internacionais em janeiro de 2023 (Rocha, 2023). Em resumo, a moeda estatal tende a sofrer uma desvalorização significativa e por uma alternativa melhor, sempre que os indivíduos tenham acesso a ela.

Além do Bitcoin, uma variedade de alternativas externas se revela como opções viáveis em contextos de crise, tais como ouro, prata, joias, itens de luxo, obras de arte e o dólar. Contudo, é crucial destacar que esses instrumentos apresentam obstáculos consideráveis, demandando um nível substancial de conhecimento prévio. Tomemos, por exemplo, o ouro e a prata, nos quais a compreensão dos graus de pureza é imperativa para assegurar transações seguras de compra e venda. No caso de itens como artigos de luxo, joias e obras de arte, cujo valor pode apreciar ao longo do tempo, é essencial possuir

conhecimento específico sobre cada objeto para conduzir negociações vantajosas.

Ademais, essas modalidades de investimento frequentemente apresentam um mercado restrito, exigindo uma extensa rede de contatos e aporte financeiro significativo, o que configura uma barreira substancial para muitos indivíduos. Por fim, embora o dólar seja amplamente considerado uma alternativa sólida em muitos países, vale ressaltar que em determinadas circunstâncias, como observado na Argentina, podem surgir controles de capitais e escassez de dólares, impedindo a aquisição para preservação de patrimônio por parte dos indivíduos e limitando as operações de importação essenciais para a continuidade dos negócios (Sousa, 2023).

Portanto, o Bitcoin se destaca de maneira singular ao abordar diversas das questões anteriormente mencionadas. No entanto, é imperativo reconhecer que seu atual processo de centralização pode comprometer significativamente esses atributos positivos. Como anteriormente observado, ao empregar o Bitcoin de maneira não convencional, ou seja, fora de sua *blockchain*, aspectos cruciais como privacidade, segurança e custódia são impactados, constituindo uma violação dos princípios fundamentais do Bitcoin. Nesse contexto, torna-se de extrema importância adotar medidas que preservem a natureza descentralizada da moeda, uma vez que a centralização, na prática, pode transformar esse ativo em uma ferramenta que se assemelha a uma moeda fiduciária.

6 O RISCO DA INEFICÁCIA DO BITCOIN

À medida que os usuários enfrentam os desafios inerentes aos limites técnicos do Bitcoin, a perspectiva da centralização emerge como um paradigma a ser considerado. A busca por soluções escaláveis deve harmonizar-se com a preservação dos princípios fundamentais que motivaram a concepção do Bitcoin. Nesse contexto, as indagações devem ser respondidas: será a centralização a única rota viável para a ampla aceitação e adoção do Bitcoin? Esse cenário torna o Bitcoin mais uma moeda fiduciária?

As evidências bibliográficas apresentadas neste estudo indicam que a arquitetura da *Lightning Network* se encontra fortemente centralizado por grandes nós de liquidez. Além disso, não se vislumbra perspectivas de melhorias tecnológicas da rede capazes de alterar esse cenário. Uma problemática adicional reside na utilização da *Lightning Network* por meio de aplicativos de instituições privadas, prática que compromete em diversos aspectos de segurança e privacidade, conforme previamente destacados. Portanto, a adoção da *Lightning Network* não se apresenta como uma solução abrangente para os desafios do Bitcoin, sendo recomendável limitar seu uso a micropagamentos.

Outra questão relevante abordada diz respeito à crescente popularização da aquisição de contratos de garantias com promessas de lastros em Bitcoins, emitidas por bancos, instituições de pagamento digital e, até mesmo, plataformas de redes sociais. Este cenário tende à realização de práticas de reservas fracionárias, ocasionando distorções no preço do ativo. À medida que a volatilidade oferta possibilidades de ganhos financeiros, os usuários tendem a buscar exposição ao ativo sem necessariamente considerar os fundamentos delineados no *whitepaper* do Bitcoin. Em última análise, os usuários renunciarão à posse efetiva do Bitcoin em favor de um contrato de garantia, transformando a utilização da criptomoeda em mais uma ferramenta sob o controle das entidades tradicionais do sistema fiduciário.

Diante das problemáticas discutidas, não se delineia um horizonte positivo para a expansão do Bitcoin como uma alternativa independente ao sistema fiduciário. A aquisição do ativo por meio de contratos está propensa a ser cada vez mais incentivada pelos principais atores do sistema financeiro. Além disso, a introdução das *CBDCs*, aliada à implementação de novas

regulamentações de controle de capital e ao aumento do rastreamento de transações financeiras, sugerem que a obtenção de Bitcoins para autocustódia por meio de corretoras formais poderá se tornar progressivamente mais desafiadora.

No entanto, caso o cenário de popularização do ativo continue a se expandir, mesmo diante da possibilidade de práticas de reserva fracionária, a crescente demanda institucional poderá resultar em uma maior escassez de Bitcoins na *blockchain* e em corretoras, influenciando de maneira significativa a precificação do ativo. Nesse contexto, os indivíduos que optam pela prática de autocustódia podem experimentar ganhos patrimoniais consideráveis ao longo do tempo.

Com isso, é crucial ressaltar que a demanda genuína pelo Bitcoin em autocustódia dificilmente perderá relevância, especialmente diante das persistentes crises econômicas do sistema fiduciário e conflitos globais. Cada vez mais, indivíduos buscam preservar seu patrimônio, motivados por questões ideológicas, estados com controle de capital rigoroso ou em situações de conflito. Assim, é plausível que as problemáticas associadas aos controles estatais, mesmo em nações mais desenvolvidas, impulsionem a adoção da prática de autocustódia. Se essa tendência se consolidar, maior será a utilidade e escassez do ativo enquanto alternativa monetária descentralizada.

Em conclusão, o Bitcoin revela-se menos eficaz como uma ferramenta descentralizada para microtransações, requerendo soluções centralizadas de segunda camada ou recorrendo a contratos fiduciários. Apesar da elevada latência e dos custos associados às transações na *blockchain*, o ativo pode desempenhar um papel relevante como uma forma de proteção patrimonial, com potencial significativo de valorização a longo prazo. Essa perspectiva, no entanto, está intrinsecamente ligada a um processo educacional individual dos usuários, necessitando que compreendam as características e benefícios da preservação do ativo em autocustódia. Caso contrário, o Bitcoin se tornará majoritariamente mais um produto financeiro de alta volatilidade controlado por instituições.

7 CONSIDERAÇÕES FINAIS

Assim como adquirir contratos de ouro em corretoras e bancos geralmente não oferecem acesso ao ouro físico, e sim uma garantia de equivalência de valor, o mesmo vem acontecendo com o Bitcoin. Ao adquirir contratos em um banco, enquanto não há a opção de saques para autocustódia em *blockchain*, o produto adquirido se torna apenas um índice volátil na composição patrimonial do usuário. Somado a isto, a popular utilização da *Lightning Network* por meio de aplicativos de terceiros também devem ocasionar diversos riscos antagônicos à própria fundamentação do Bitcoin.

Conforme discutido, o curso natural do Bitcoin, derivado da sua atual arquitetura e uso generalizado, tende a torná-lo um ativo escasso, controlado por poucas instituições e chefiadas por entidades governamentais. Assim, cabe aos usuários finais a crucial decisão de adotar a criptomoeda apenas como um ativo de risco terceirizado ou por obter soberania patrimonial por meio de práticas descentralizadas. Ao optar pelo caminho da liberdade, se faz necessário que haja um processo educacional que oriente o indivíduo a ser o responsável direto pelo seu patrimônio, ou seja, ser seu próprio banco.

Nesse caminho, se faz crucial a adoção de carteiras de autocustódia, nas quais os usuários detêm total controle e responsabilidade sobre suas chaves privadas. A tecnologia *blockchain* viabiliza que cada indivíduo possa possuir sua própria carteira privada, requerendo apenas o conhecimento adequado sobre configurações e segurança de senhas. Essa abordagem coloca nas mãos dos usuários a gestão direta de seus ativos, fortalecendo a segurança e a preservação dos princípios descentralizados do Bitcoin.

Duas formas de realizar a autocustódia são comumente recomendadas sendo elas a utilização de uma carteira *Hot Wallet* ou *Cold Wallet*. Uma *Hot Wallet* tem conexão com a internet, utilizada por um programa no computador ou smartphone do usuário, que irá armazenar as chaves privadas. Por possuir exposição à internet, há riscos substanciais de invasão de dados por ataques cibernéticos, no qual invasores podem acessar seu dispositivo por meio de alguma vulnerabilidade de uso e roubar suas chaves privadas. Portanto, se faz necessário a adoção de medidas preventivas de segurança digital nos dispositivos. Uma *Cold Wallet*, por outro lado, não possui conexão direta com a

internet. Geralmente utilizada por um dispositivo físico que armazena as chaves privadas. Assim, é possível mitigar os riscos de invasões de hackers, pois não há conectividade com internet.

Além da autocustódia, existem alternativas de obtenção de Bitcoins de forma descentralizada. Denominadas transações *peer-to-peer (P2P)*, é necessário a obtenção de contato direto com usuários interessados em vender o ativo. Diversos são os grupos de mensageiros, fóruns virtuais e sites que concentram esses vendedores. Destacam-se por questões organizacionais e de segurança os serviços de *marketplace (*mercados virtuais), que concentram compradores e vendedores, ranqueando-os por sistemas de reputação e *feedbacks*. Por se tratar de uma modalidade que necessita confiança, é necessário pesquisar muito bem a reputação do vendedor. Além dos ambientes virtuais, diversos são os eventos que concentram vendedores e compradores para a negociação de forma presencial, geralmente em estabelecimentos comerciais como *shoppings centers* e cafeterias.

Em linhas gerais, o controle sobre a própria carteira capacita os indivíduos a preservarem elementos essenciais do Bitcoin, como privacidade e segurança, eliminando a necessidade de depender de terceiros. Ao promover ativamente o uso de carteiras de autocustódia, é possível atingir os princípios fundamentais do Bitcoin de maneira mais eficaz por parte dos usuários. Diversos métodos de geração de chaves estão disponíveis, acompanhados por uma ampla gama de alternativas e funcionalidades de carteiras. Portanto, é imperativo que os usuários invistam tempo para compreender os aspectos cruciais de segurança envolvidos nesse processo.

Adicionalmente, é fundamental que a comunidade acadêmica e os desenvolvedores se dediquem à busca por aprimoramentos tecnológicos e soluções tanto para a *blockchain* primária quanto secundárias, bem como para o desenvolvimento de carteiras de autocustódia mais seguras. Esse esforço conjunto visa impulsionar uma cultura digital cada vez mais livre, alinhada com os princípios fundamentais de descentralização que Satoshi Nakamoto introduziu por meio dessa tecnologia.

8 REFERÊNCIAS BIBLIOGRÁFICAS

99BITCOIN. Bitcoin Obituaries - "Bitcoin is Dead" Declared 400+ Times. 2023. Disponível em: https://99bitcoins.com/bitcoin-obituaries/. Acesso em: 25 out. 2023.

ABDALLA, R. A evolução dos meios de pagamento, da pré-história à Internet das Coisas. Canaltech, 2017. Disponível em: https://arquivo.canaltech.com.br/mercado/a-evolucao-dos-meios-de-pagamento-da-pre-historia-a-internet-das-coisas-97812/.

AGGIO, G. O. Moeda, convenção, contratos e impostos: uma contribuição para a teoria da aceitabilidade da moeda. 2008. 145 f. Dissertação (Mestrado) — Curso de Ciências Econômicas, Departamento de Instituto de Economia, Universidade Estadual de Campinas, Campinas, 2008. Disponível em: http://www.eco.unicamp.br/docdownload/monografias/Gustavo_de_Oliveira_Aggio.pdf

AMMOUS, S. The Bitcoin Standard: The Decentralized Alternative to Central Banking. 1 ed. Wiley, 2018.

ANTONOPOULOS, A. M.; OSUNTOKUN, O.; PICKHARDT, R. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. 1 ed. Califórnia: O'Reilly Media, 2022.

ARISTOTLE. Aristotle in 23 Volumes. Vol. 21. Cambridge, MA, Harvard University Press; London, William Heinemann Ltd. 1944. Disponível em: http://data.perseus.org/citations/urn:cts:greekLit:tlg0086.tlg035.perseus-eng1:1.1257a.

BAGUS, P. A origem do dinheiro e o trágico caminho até o euro. Mises Brasil, 2011. Disponível em: https://mises.org.br/article/1191/a-origem-do-dinheiro-e-o-tragico-caminho-ate-o-euro.

BAINS, P. *et al*. Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. FinTech Notes. Setembro, 2022. Disponível em: https://www.elibrary.imf.org/view/journals/063/2022/007/article-A001-en.xml?ArticleTabs=abstract.

BANCO CENTRAL DO BRASIL. DREX — Real Digital. 2023. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/drex.

BANCO CENTRAL DO BRASIL. Origin and Evolution of Money. 2004. Disponível em: https://www.bcb.gov.br/ingles/origevoli.asp?frame=1.

BARAN, P. On Distributed Communications Networks. Santa Monica, CA: RAND Corporation, 1962. Disponível em: https://doi.org/10.7249/P2626.

BARRETO, P. H. História - Bretton Woods. Quarenta e quatro paises, inclusive o Brasil, participaram da reunião em New Hampshire (EUA): o mundo vivia a ressaca da crise de 1929, seguida da Segunda Guerra Mundial. Instituto de Pesquisa Econômica Aplicada, 2009. Disponível em: https://www.ipea.gov.br/desafios/index.php?option=com_content&view=article&id=2247:catid=28&Itemid=23.

BELTRÃO, H.; GELLER, A. Há 52 anos, o que restava do padrão-ouro era abolido, dando lugar ao papel-moeda estatal. Mises Brasil, 2023. Disponível em: https://mises.org.br/artigos/3054/ha-52-anos-o-que-restava-do-padrao-ouro-era-abolido-dando-lugar-ao-papel-moeda-estatal.

BERTOLUCCI, G. Jericoacoara estabelece o recorde mundial de pagamentos com Bitcoin. 2023. Disponível em: https://livecoins.com.br/jericoacoara-estabelece-o-recorde-mundial-de-pagamentos-com-bitcoin/.

BITCOIN WIKI. For all your Bitcoin information needs. 2010. Disponível em: https://bitcoin.it.

BITNODES. REACHABLE BITCOIN NODES. Disponível em: https://bitnodes.io/. Acesso em: 06 de setembro de 2023.

BLUDNIK, I. Central Bank Digital Currency and the Cashless Economy: The African Experience. vol XXVI. European Research Studies Journal, 2023. Disponível em: https://ideas.repec.org/a/ers/journl/vxxviy2023i3p314-324.html.

BOYAPATI, V. The Bullish Case for Bitcoin. 1 ed. 2021

CAMILO, G. F. *et al*. Análise da Evolução Topológica da Rede Lightning de Canais de Pagamento. Porto Alegre: Sociedade Brasileira de Computação, 2022. Disponível em: https://doi.org/10.5753/sbseg.2022.225320.

CARDOSO, B. O que é “gasto duplo” e como o Bitcoin é capaz de evitá-lo?. 2018. Disponível em: https://jus.com.br/artigos/66683/o-que-e-gasto-duplo-e-como-o-bitcoin-e-capaz-de-evita-lo.

CAVALLINI, M. Auxílio Brasil: estou na fila, quais são os critérios de aprovação? G1, 2021. Disponível em: https://g1.globo.com/economia/noticia/2021/11/23/auxilio-brasil-estou-na-fila-quais-sao-os-criterios-de-aprovacao.ghtml

CHOHAN, U. W. FTX, Sam Bankman-Fried, and the Cryptoexchange Problem. Janeiro, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4326161.

CNN BRASIL. China proíbe mineração e declara ilegais transações com criptomoedas no país. 2023. Disponível em https://www.cnnbrasil.com.br/economia/china-amplia-restricoes-e-proibe-mineracao-de-criptomoedas-em-todo-o-pais/. Acesso em: 25 out. 2023.

COINMAP. 2023. Disponível em: https://coinmap.org/view/#/world/56.21892319/-15.24902344/3. Acesso em: 03 set. 23.

COREPAY. 2021. Cashless Societies: Which Countries Are Making The Switch? Disponível em: https://corepay.net/articles/cashless-countries/.

CROMAN, K.; *et al*. On Scaling Decentralized Blockchains. Financial Cryptography and Data Security. vol. 9604. P. 106–125. Agosto, 2016. Disponível em: https://doi.org/10.1007/978-3-662-53357-4_8.

CYSNE, R. P. Imposto Inflacionário e Transferências Inflacionárias no Brasil. Brazilian Jornal of Policial Economy. vol. 14. p. 463–470. Maio, 1994. Disponível em: https://doi.org/10.1590/0101-31571994-0784.

DASAKLIS, T. K.; MALAMAS, V. A Review of the Lightning Network's Evolution: Unraveling Its Present State and the Emergence of Disruptive Digital Business Models. Journal of Theoretical and Applied Electronic Commerce Research. vol. 18. P. 1338–1364. Agosto, 2023. Disponível em: https://www.mdpi.com/0718-1876/18/3/68.

DUPUIS, D. Money laundering in a CBDC World: A Game of Cats and Mice. American University of Sharjah - School of Business and Management, 2021. Disponível em http://dx.doi.org/10.2139/ssrn.3793713.

EUROPEAN SECURITIES AND MARKETS AUTHORITY. MARKETS IN CRYPTO-ASSETS REGULATION (MiCA). 2023. Disponível em: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica.

FILHO, M. B. O. Utilizando o protocolo bitcoin para condução de computações multilaterais seguras e justas. Dissertação (Mestrado) — Programa de Pós-graduação em Ciência da Computação, Universidade Federal de Pernambuco, 2016. Disponível em: https://repositorio.ufpe.br/handle/123456789/17143.

FISHER, I. A Teoria do Juro: Determinada pela impaciência por gastar renda e pela oportunidade de investi-la. São Paulo: Nova Cultural, 1986.

FOURTANÉ, S. Sweden: How to Live in the World's First Cashless Society. Interesting Engineering, 2023. Disponível em: https://interestingengineering.com/innovation/sweden-how-to-live-in-the-worlds-first-cashless-society.

G1. Lei Marcial: homens ucranianos e naturalizados com idade de 18 a 60 anos estão proibidos de sair da Ucrânia. 2022. Disponível em: https://g1.globo.com/mundo/noticia/2022/02/25/lei-marcial-homens-ucranianos-e-naturalizados-com-idade-de-18-a-60-anos-estao-proibidos-de-sair-da-ucrania.ghtml. Acesso em: 25 out. 2023.

GIL, A. C.; *et al*. Como elaborar projetos de pesquisa. São Paulo: Atlas, 2002.

GREMAUD, A. P.; *et al*. Manual de Economia. 5. ed. São Paulo: Saraiva, 2004.

HAFID, A.; HAFID, A. S.; SAMIH, M. Scaling Blockchains: A Comprehensive Survey. Vol. 8. IEEE, 2020. Disponível em: https://ieeexplore.ieee.org/document/9133427.

HAYEK, F. A. V. Desestatização Do Dinheiro. São Paulo: LVM Editora, 2011.

HERRERA-JOANCOMARTÍ, J.; PÉREZ-SOLÀ, C. Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions. International Conference on Modeling Decisions for Artificial Intelligence. vol. 9880. Mês, 2016. Disponível em: https://doi.org/10.1007/978-3-319-45656-0_3.

HONORATO, S. Nubank não vai permitir saque de bitcoin comprado pelo aplicativo. Portal do Bitcoin, 2022. Disponível em: https://portaldobitcoin.uol.com.br/nubank-nao-vai-permitir-saque-de-bitcoin-comprado-pelo-aplicativo/.

HU, Y.; *et al*. Security Threats from Bitcoin Wallet Smartphone Applications: Vulnerabilities, Attacks, and Countermeasures. Eleventh ACM Conference on Data and Application Security and Privacy. P. 89–100. Abril, 2021. Disponível em: http://dx.doi.org/10.1145/3422337.3447832.

IBRACHINA. Invenções chinesas: dinheiro. 2023. Disponível em: https://www.ibrachina.com.br/invencoes-chinesas-dinheiro. Acesso em: 21 nov. 2023.

IMBERT,F. *BlackRock* CEO Larry Fink calls bitcoin an ‘index of money laundering’. CNBC, 2017. Disponível em: https://www.cnbc.com/2017/10/13/blackrock-ceo-larry-fink-calls-bitcoin-an-index-of-money-laundering.html. Acesso em: 25 out. 2023.

INVESTING. Bitcoin quase dobra de valor desde o topo histórico na Argentina. 2023. Disponível em: https://br.investing.com/news/cryptocurrency-news/bitcoin-quase-dobra-de-valor-desde-o-topo-historico-na-argentina-1168957. Acesso em: 26 out. 2023.

JENKINSON, G. Índia, Nigéria e Tailândia lideram o Índice Global de Adoção de Criptomoedas de 2023 da Chainalysis. Cointelegraph, 2023. Disponível em: https://br.cointelegraph.com/news/india-tops-chainalysis-2023-global-crypto-adoption-index. Acesso em: 26 out. 2023.

KALOUDIS, G. China não freia mineração de Bitcoin um ano após banimento. Infomoney, 2022. Disponível em: https://www.infomoney.com.br/mercados/china-nao-freia-mineracao-de-bitcoin-um-ano-apos-banimento/. Acesso em: 25 out. 2023.

LIN, J. H.; *et al*. Lightning network: a second path towards centralisation of the Bitcoin economy. New Journal of Physics. Vol. 22. agosto, 2020. Disponível em: https://dx.doi.org/10.1088/1367-2630/aba062.

LOOKINTOBITCOIN. Bitcoin: Addresses with Balance > 1 BTC. 2023. Disponível em: https://www.lookintobitcoin.com/charts/addresses-greater-than-1-btc/. Acesso em: 03 set. 23.

LOPES, J. C.; ROSSETTI, J. P. Economia Monetária. 9. ed. São Paulo: Atlas, 2005.

LYNCH, D. C; LUNDQUIST, L. Digital Money: the new era of internet commerce. 1 ed. Canada: John Wiley & Sons, Inc, 1996.

MALAR, J. P. CEO da *BlackRock*, Larry Fink diz que bitcoin é "ouro digital" e defende ativo. Exame, 2023. Disponível em: https://exame.com/future-of-money/ceo-blackrock-larry-fink-bitcoin-ouro-digital-defende-ativo/. Acesos em: 24 out. 2023.

MALHOTRA, *et al*. How Blockchain Can Automate KYC: Systematic Review. 2021. Disponível em: https://doi.org/10.1007/s11277-021-08977-0.

MARINS, L. G. Polícia de Israel congela contas do Hamas na exchange de criptomoedas Binance. Infomoney, 2023. Disponível em:

https://www.infomoney.com.br/onde-investir/policia-de-israel-congela-contas-do-hamas-na-exchange-de-criptomoedas-binance/

MARKETSANDMARKET. Coinbase, Inc. (US) and Gemini Trust Company, LLC. (US) are leading players in Crypto Asset Management Market. 2021. Disponível em: https://www.marketsandmarkets.com/ResearchInsight/crypto-asset-management-market.asp. Acesso em: 03 set. 23.

MARTING, N. Venezuelanos recorrem a criptomoedas contra hiperinflação. DW, 2021. Disponível em: https://www.dw.com/pt-br/venezuelanos-recorrem-a-criptomoedas-contra-hiperinfla%C3%A7%C3%A3o/a-57269576. Acesso em: 26 out. 2023.

MCELROY, W. Revolução Satoshi: A Revolução das Esperanças Crescentes. 1. ed. Editora Konkin, 2022.

MÉLIUZ. Como comprar bitcoins sem taxas? 2023. Disponível em: https://www.meliuz.com.br/blog/como-comprar-bitcoin-sem-taxas/

METRI, M. M. Acumulação de poder, sistemas e territórios monetários: uma análise teórica sobre a natureza da moeda e sua relação com a autoridade central. v. 33, n. 2. Ensaios FEE, 2012. Disponível em: http://200.198.145.164/index.php/ensaios/article/view/2571.

MISES, L. V. The Theory of Money and Credit. 3. ed. New Haven: Yale University Press, 1953.

MITCHELHILL, T. X de Elon Musk se aproxima de pagamentos com criptomoedas com obtenção de nova licença estadual. Cointelegraph, 2023. Disponível em: https://br.cointelegraph.com/news/x-twitter-crypto-payments-rhode-island-licence

MOOKERJEE, A. S. What If Central Banks Issued Digital Currency? Harvard Business Review, 2021. Disponível em: https://hbr.org/2021/10/what-if-central-banks-issued-digital-currency.

NAIR, V.; SONG, D. Decentralizing Custodial Wallets with MFKDF. International Conference on Blockchain and Cryptocurrency (ICBC). Maio, 2023. Disponível em: http://dx.doi.org/10.1109/ICBC56567.2023.10174998.

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Eletronic Cash System. 2008. Disponível em: https://bitcoin.org/bitcoin.pdf.

NUBANK. Nubank Cripto: passo a passo para comprar criptomoedas no app do Nu. 2022. Disponível em: https://blog.nubank.com.br/nubank-cripto-como-comprar-criptomoedas-no-app/.

ORRELL, D; CHLUPATÝ, R. The evolution of money. 1. ed. Nova York: Columbia University Press, 2016.

PACKER, A. FedNow Is Here – and a CBDC Is Coming. Palm Beach Research Group, 2023. Disponível em: https://www.palmbeachgroup.com/palm-beach-daily/fednow-is-here-and-a-cbdc-is-coming/.

PAL, R. A grande mudança monetária e bancária que está por vir — está preparado? Mises Brasil, 2021. Disponível em: https://mises.org.br/artigos/3006/a-grande-mudanca-monetaria-e-bancaria-que-esta-por-vir-esta-preparado.

PEDRO, C. Refugiados ucranianos que trabalham com criptos encontram segurança em Portugal. Jornal de Negócios, 2022. Disponível em: https://www.jornaldenegocios.pt/economia/europa/invasao-da-ucrania/detalhe/refugiados-ucranianos-que-trabalham-com-criptos-encontram-seguranca-em-portugal. Acesso em: 25 out. 2023.

POON, J.; THADDEUS, D. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. 2016. Disponível em: https://lightning.network/lightning-network-paper.pdf.

REVERTER, B. R. Economia 3.0: do escambo até as finanças descentralizadas. 1 ed. Paraíba: Borja Ruiz Reverter, 2020.

RIARD, A.; NAUMENKO, G. Time-Dilation Attacks on the Lightning Network. 2020. Disponível em: https://arxiv.org/abs/2006.01418.

ROCHA, LUCIANO. Preço do Bitcoin se aproxima dos US$ 40 mil na Nigéria; entenda. Criptofácil, 2023. Disponível em: https://www.criptofacil.com/preco-do-bitcoin-se-aproxima-dos-us-40-mil-na-nigeria-entenda/. Acesso em: 25 out. 2023.

ROTHBARD, M. N. O que o Governo Fez Com o nosso Dinheiro?. 1 ed. São Paulo: Instituto Ludwig von Mises, 2013.

RUBINSTEINS, L. *BlackRock* anuncia que vai começar a comprar Bitcoin. Blocktrends, 2023. Disponível em: https://blocktrends.com.br/blackrock-anuncia-que-vai-comecar-a-comprar-bitcoin/. Acesso em: 24 out. 2023

SABRY, F. Digital Currency. ed 1. One Billion Knowledgeable, 2021.

SMITH, A. A Riqueza das Nações. 1 ed. São Paulo: Abril Cultural, 1996.

SOTO, J. H. Moeda, crédito bancário e ciclos econômicos. 1 ed. São Paulo: Instituto Ludwig von Mises, 2012.

SOUSA, R. Dólar evapora da Argentina: 3 dados para entender a crise no país — e por que a situação do Brasil é bem melhor que a dos “hermanos”. Seu Dinheiro, 2023. Disponível em: https://www.seudinheiro.com/2023/bolsa-dolar/dolar-argentina-brasil-crise-rens/. Acesso em: 26 out. 2023.

STASI, G. D.; *et al*. Routing Payments on the Lightning Network. IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data. P. 1161–1170. Agosto, 2018. Disponível em: https://ieeexplore.ieee.org/document/8726489.

THE GUARDIAN. Riots erupt in Nigerian cities as bank policy leads to scarcity of cash. 2023. Disponível em: https://www.theguardian.com/world/2023/feb/15/angry-protests-erupt-across-nigeria-against-scarcity-of-cash.

ULRICH, F. Bitcoin: A Moeda Na Era Digital. 1 ed. São Paulo: Instituto Ludwig von Mises, 2014.

VASCONCELOS, W. R. A. Interferência estatal e moeda: o papel do bitcoin. 2021. 35 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Econômicas) — Departamento de Economia, Universidade Federal Rural de Pernambuco, Recife, 2021. Disponível em: https://repository.ufrpe.br/handle/123456789/3936.

VIEIRA, J. P. "A História do Dinheiro". Lisboa: Academia das Ciências de Lisboa. Conferências e Seminários, Instituto de Altos Estudos. Março, 2017. Disponível em: < https://doi.org/10.58164/20ev-0760>.

WALICZEK, S. What are central bank digital currencies and what could they mean for the average person? World Economic Forum, 2023. Disponível em: https://www.weforum.org/agenda/2023/10/what-are-central-bank-digital-currencies-advantages-risks/.

WARD, O.; ROCHEMONT, S. Understanding Central Bank Digital Currencies (CBDC). Institute and Faculty of Actuaries. 2019. Disponível em: https://www.actuaries.org.uk/system/files/field/document/Understanding%20CBDCs%20Final%20-%20disc.pdf.

WOLFFENBÜTTEL, A. O que é? — Índice de Gini. Desafios do Desenvolvimento — Instituto de Pesquisa Econômica Aplicada. ed. 4. novembro, 2004. Disponível em: https://www.ipea.gov.br/desafios/index.php?option=com_content&id=2048:catid=28.

WOODS, T. E. The Great Gold Robbery of 1933. Mises Institute, 2022. Disponível em: https://mises.org/library/great-gold-robbery-1933.

YCHARTS. Bitcoin Average Transaction Fee. 2023. Disponível em: https://ycharts.com/indicators/bitcoin_average_transaction_fee. Acesso em: 03 set. 23.

ZABKA, P. *et al*. A Centrality Analysis of the Lightning Network. Financial Cryptography and Data Security. vol. 12399. P. 105–119. Janeiro, 2021. Disponível em: https://doi.org/10.1007/978-3-031-18283-9_18.

ZANATTA, P. Entenda como as criptomoedas estão sendo usadas na guerra entre Ucrânia e Rússia. CNN Brasil, 2022. Disponível em: https://www.cnnbrasil.com.br/economia/entenda-como-as-criptomoedas-estao-sendo-usadas-na-guerra-entre-ucrania-e-russia/. Acesso em: 25 out. 2023.