UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO ACADÊMICO DO AGRESTE
NÚCLEO DE GESTÃO
CURSO DE CIÊNCIAS ECONÔMICAS

JOSÉ ALVES DE MELO JÚNIOR

Bitcoin: Tecnologias subjacentes, suas aplicações no mercado e um debate acerca da função das criptomoedas na sociedade contemporânea

Caruaru
2025

JOSÉ ALVES DE MELO JÚNIOR

Bitcoin: Tecnologias subjacentes, suas aplicações no mercado e um debate acerca da função das criptomoedas na sociedade contemporânea

Trabalho de Conclusão do Curso apresentada à Universidade Federal de Pernambuco, como requisito para a como requisito parcial para obtenção do grau de Bacharel em Ciências Econômicas.

Área de concentração: Economia.

Orientador (a): Profª. Drª. Lucilena Ferraz Castanheira Corrêa

Caruaru
2025

AGRADECIMENTOS

Agradeço, em primeiro lugar, aos meus pais, pelo incentivo constante ao estudo ao longo dos anos, e, sobretudo, por terem me criado sobre valores morais sólidos. Esses fundamentos foram essenciais para que eu pudesse abordar com profundidade e discernimento os temas aqui desenvolvidos, permitindo-me ir além da técnica e alcançar a reflexão crítica.

Estendo minha sincera gratidão à Profª. Drª. Lucilena, por sua orientação atenta, pelo apoio técnico e pela confiança durante o desenvolvimento deste trabalho. Sua escuta generosa e seus apontamentos precisos foram decisivos para que esta pesquisa alcançasse consistência e clareza.

Sou igualmente grato a todos os professores que me acompanharam ao longo da graduação, pois foram eles que, com dedicação e excelência, me proporcionaram as bases técnicas e analíticas necessárias para desenvolver a mentalidade de um economista, ampliando minha capacidade crítica e interpretativa diante dos desafios contemporâneos.

Por fim – e acima de tudo – agradeço a Deus, cuja providência tem guiado silenciosamente cada passo do meu caminho, abrindo portas, iluminando decisões e moldando minha trajetória tanto no plano profissional quanto na minha formação como homem.

Vento e Liberdade

"São morros e colinas verdejantes,
De perto sopra o vento sobre a grama,
Ondas verdes vistas do mirante,
Mundos se movem ao vento e a quem ama.

No sopro do vento canta a liberdade
– Um sussurro na alma e no coração.
Flechas do Sol raiam outra dimensão,
Nuvens brancas cortejam a verdade.

Voa a águia entre o branco e azul,
Como alma liberta da farsa humana.
O mundo tudo promete, mas só engana.

Pesa a máscara, é leve a verdade.
Sou. Fico. Que morra a falsidade!
Sou quem sou, livre sob Cruz do Sul."

José Alves de Melo Júnior (Autoria própria)

Bitcoin: Tecnologias subjacentes e um debate acerca da função das criptomoedas na sociedade contemporânea

Bitcoin: Underlying Technologies and a Debate on the Role of Cryptocurrencies in Contemporary Society

José Alves de Melo Júnior[1]

RESUMO

Este trabalho tem como objetivo analisar o desenvolvimento técnico da criptografia aplicada ao Bitcoin e às tecnologias subjacentes do sistema blockchain, ressaltando suas aplicações no mercado e seus impactos econômicos. A pesquisa parte da concepção do Bitcoin por Nakamoto (2008), considerado o marco inicial das finanças descentralizadas (DeFi), e examina o papel do blockchain como inovação capaz de proporcionar um sistema descentralizado, seguro e transparente. A metodologia adotada baseia-se em revisão bibliográfica e documental, com suporte em artigos acadêmicos, livros especializados e fontes digitais. O estudo discute as implicações do uso de criptomoedas, especialmente no setor financeiro, abordando os dilemas em torno da volatilidade, da segurança e da necessidade de regulação. Nesse sentido, enfatiza-se o debate entre correntes que defendem a liberdade monetária e a descentralização e aquelas que ressaltam a importância do controle estatal e da regulação internacional. Conclui-se que o impacto e o legado das criptomoedas no mundo contemporâneo dependerão da capacidade de equilibrar inovação tecnológica com estabilidade macroeconômica, liberdade com responsabilidade e descentralização com governança eficaz. Cabendo aos economistas compreenderem esse fenômeno em sua complexidade. Nas palavras de Hayek, trata-se de um "fenômeno complexo".

Palavras-chave: Blockchain, Descentralização, Criptografia

ABSTRACT

This study aims to analyze the technical development of cryptography applied to Bitcoin and the underlying technologies of the blockchain system, highlighting their market applications and economic impacts. The research begins with the conception of Bitcoin by Nakamoto (2008), considered the starting point of decentralized finance (DeFi), and examines the role of blockchain as an innovation capable of providing a decentralized, secure, and transparent system. The methodology is based on bibliographic and documentary review, supported by academic articles, specialized books, and reliable digital sources. The study discusses the implications of

[1] Graduando em Ciências Econômicas pela Universidade Federal de Pernambuco e e-mail: josealves.melojunior@ufpe.br

cryptocurrency use, especially in the financial sector, addressing the dilemmas surrounding volatility, security, and the need for regulation. In this regard, it emphasizes the debate between those who advocate monetary freedom and decentralization and those who stress the importance of state control and international regulation. The conclusion is that the impact and legacy of cryptocurrencies in the contemporary world will depend on the ability to balance technological innovation with macroeconomic stability, freedom with responsibility, and decentralization with effective governance. It is up to economists to understand this phenomenon in its complexity. In Hayek's words, it is a "complex phenomenon".

Keywords: Blockchain; Decentralization; Cryptography

DATA DE APROVAÇÃO: 21 de Julho de 2025.

1 INTRODUÇÃO

O sistema econômico mundial, a partir do ano de 2009, começa a sofrer alterações a partir da implementação e comercialização de um novo ativo nas mediações financeiras, as chamadas criptomoedas. “No ano de 2009, foi criada a primeira criptomoeda, o Bitcoin, que é um sistema de caixa eletrônico que liga um ponto a outro e permite o envio de pagamentos diretos sem passar por instituições financeiras” (DE SENNA, SOUZA; 2023, p.2).

Diante dessa perspectiva**,** o Bitcoin nasceu da aspiração de desenvolver um método de pagamento descentralizado na internet, permitindo que as transações fossem permanentes e eliminando a possibilidade de duplicação de pagamentos. Em síntese, o Bitcoin tem como objetivo oferecer um sistema de pagamento *peer-to-peer* (entre pares), rejeitando a intervenção de intermediários para a validação ou o registro das transações. É importante ressaltar que essa inovação monetária foi criada por Satoshi Nakamoto – um pseudônimo que pode se referir a um indivíduo ou a um grupo de programadores, cuja verdadeira identidade permanece desconhecida.

Baur et al. (2018, p.177), corrobora que a criptomoeda tem entre suas funções, a de demanda. Ou seja, pode ser utilizada como reserva de valor que, “por definição, criptomoeda é uma moeda alternativa, entretanto é um híbrido de moeda mercadoria e moeda fiduciária, determinado por uma regra determinística automática cumprida pela mineração competitiva semelhante ao dinheiro commodity, como o ouro, mas sem valor intrínseco”.

Segundo Liang; Li; Zeng (2018), ressaltam que as transações em criptomoedas, por se apresentar como uma nova forma de transações e modelos de ativos, pode-se afirmar que apresenta um forte apelo para se colocar como uma alternativa a moeda fiduciária tradicional.

> Quando este artigo foi escrito, havia mais de 900 moedas no mercado de criptomoedas e o valor total de mercado ultrapassou US$ 578 bilhões. Assim, é o momento certo para investigá-los e compará-los, de modo a entender completamente a criptomoeda e fornece uma base para pesquisas futuras (Liang; Li; Zeng, 2018,p.1)

Fortuna; Holtz; Neff (2013) corroboram no seu estudo, que embora a rede de transações Bitcoin na época estava iniciando como centro de estudo por ser relativamente nova, ela já exibia várias qualidades à medida que era desenvolvida.

No lado diametralmente oposto, pode-se citar a ressalva de Mattos, Abouchedid, Araújo e Silva (2018,p.775), para lançar a luz a discussão acerca da criptomoeda.

> Usando o Bitcoin como exemplo, essa criptomoeda não é reserva de valor, já que seu valor não se mostrou estável ao longo do tempo. Não é universalmente aceito como meio de troca, e também não é unidade de conta. Bitcoins têm elasticidade de produção baixa, uma vez que dependem de "mineração", mas sua elasticidade de substituição é alta, sendo sua demanda facilmente substituída entre as demais criptomoedas e também entre outros ativos.

Diante dessa perspectiva, ao lançar o paper intitulado "Bitcoin: A *Peer-to-Peer Electronic Cash System*" (Nakamoto, 2008), o autor descreve as tecnologias e conceitos fundamentais que sustentam o Bitcoin e seu Blockchain[2], referindo-se ao livro-razão descentralizado que usa blocos encadeados para registrar transações. Entre os conceitos abordados, destacam-se o blockchain, as funções hash[3] e o mecanismo de *proof-of-work* (PoW)[4] .

> Acompanhar a evolução das variáveis, como criptomoedas, é importante para que seja possível interpretar e antecipar mudanças no mercado, os impactos para o sistema econômico e para a geração de conhecimento na área. Estudar a relação de um novo ativo inserido junto ao mercado tradicional é importante porque pode gerar informação sobre como o mercado se comporta perante novos ativos. Novos tipos de ativos podem surgir a qualquer momento; como eles vão se comportar diante do mercado já consolidado e qual a influência que esse mercado pode sofrer são incógnitas importantes de serem acompanhadas para a evolução das teorias econômicas envolvidas e para melhorar a tomada de decisão por parte de investidores (DE SENNA, SOUZA; 2023, p.2)

Dessa maneira, esse estudo tem como objetivo central, trazer a luz o papel do Bitcoin, as tecnologias subjacentes e sua aplicação no mercado, levantando uma discussão acerca do seu papel na sociedade atual. A partir dos conceitos inaugurais mencionados anteriormente, o presente trabalho tem como objetivos específicos:

---

[2] *Blockchain* é um termo que significa uma combinação das palavras "*block*" (bloco) e "*chain*" (corrente).
[3] Uma função *hash* é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.
[4] O *Proof of Work* é um algoritmo de consenso no qual é caro e demorado produzir uma parte dos dados, mas é fácil para outras pessoas verificarem se os dados estão corretos.

a) Apresentar as tecnologias que compõem o ecossistema *blockchain* e discutir suas aplicações práticas, com foco especial no contexto das criptomoedas;

b) Expor uma discussão acerca do Bitcoin e suas perspectivas como uma moeda digital no mundo financeiro, levantando a questão sobre inovação ou controle estatal.

A estrutura do estudo será apresentada em quatro seções. O primeiro se refere a esta introdução, que em linhas gerais discorre sobre os aspectos principais que norteiam a atual pesquisa. No tópico dois apresentará as inovações tecnológicas subjacentes no sistema das criptomoedas. Na seção seguinte, a seção buscará abordar as discussões a respeito do papel das criptomoedas no sistema financeiro contemporâneo e por conseguinte a finalização, discorrerá sobre à guisa de conclusão desta pesquisa.

2 REDES DE INOVAÇÕES INTRÍSICA NO SISTEMA DA CRIPTOMEDA

A partir dos conceitos que compõem uma rede de inovações, busca-se apresentar as tecnologias que fazem parte do ecossistema blockchain e discutir suas aplicações na prática, com destaque para o universo das criptomoedas. Para isso, utilizamos uma abordagem de pesquisa que envolve revisão de livros, artigos acadêmicos e fontes digitais confiáveis.

2.1 Ecossistema *Blockchain*

As inovações tecnológicas de uma rede *blockchain* são cruciais para entender a própria rede, logo que os principais aspectos tecnológicos foram arquitetados para atender os valores centrais que balizam o ecossistema *blockchain* como descentralização, autonomia, privacidade e inovação. São tecnologias que já foram pensadas ou desenvolvidas por outros pesquisadores e entusiastas, mas a genialidade de Nakamoto (2008) foi a maestria da junção destas em uma rede descentralizada funcional. Diante dessa perspectiva, o *blockchain*, se apresenta como uma tecnologia fundamental por trás do Bitcoin, evoluiu a partir de conceitos anteriores de dinheiro digital e criptografia.

Uma das referências iniciais mencionadas por Satoshi Nakamoto (2008) em seu trabalho seminal é o conceito de *B-money*, proposto por Wei Dai em 1993. O *B-money* aparece como uma concepção inovadora, resultado do movimento *cyber*-anarquista[5], que se dedicava a encontrar

[5] Movimento que entendia que através da liberdade cibernética (internet), conseguir-se-ia impactar nas formas autoritárias de Estado (Luiz Felipe Pondé – Jornal da Cultura, 11/12/21).

alternativas para o desenvolvimento de um sistema monetário digital totalmente autônomo em relação a governos ou empresas. Esta iniciativa representa uma abordagem pioneira na criação de uma moeda digital descentralizada, onde a emissão de dinheiro não estaria sob o controle de qualquer entidade central. Ademais, o *B-money* traz pela primeira vez a ideia de geração monetária fundamentada no esforço computacional, que mais tarde se tornaria o que conhecemos como mecanismo de *proof-of-work (PoW*).

O conceito de *PoW* está inserido numa ideia central para a proposta de Dai e, posteriormente, para o desenvolvimento do Bitcoin. Ele estabelece que qualquer modificação no sistema requer a realização de trabalho computacional significativo, um processo que demanda recursos e energia. Essa exigência de esforço computacional cria um custo inerente às alterações no sistema, desencorajando ataques em larga escala. No caso de um ataque massivo, o agente malicioso teria que arcar com custos computacionais exorbitantes, tornando tais ações economicamente inviáveis. Assim, defende GERVAIS, Arthur et al (2016) que o *PoW*, tal como na concepção inicial de Nakamoto (2008), funciona como um mecanismo de segurança, protegendo a rede contra comportamentos desonestos ou maliciosos, valendo-se de um sistema de consenso de rede, com agentes egoístas[6], amparados pelas regras *a priore* que sustentam o funcionamento da *blockchain*.

Em suma, o *B-money* representa um esforço intelectual fundamental que pavimentou o caminho para o desenvolvimento do Bitcoin e da tecnologia *blockchain*. Ele antecipou muitas das questões e soluções que hoje definem o universo das criptomoedas, como a descentralização, a segurança baseada em custos computacionais e a validação de ações por meio de algoritmos consensuais. Assim, o legado de Wei Dai e sua visão *cyber*-anarquista continua a reverberar no ecossistema das moedas digitais, inspirando inovações e fortalecendo a ideia de um sistema financeiro mais livre, descentralizado e resistente à manipulação.

Sendo descritos por Wei Dai (1993) dois tipos de protocolo para que seja viável o sistema de transações:

1) No primeiro depende de um canal de transmissão anônimo síncrono e ininterrupto, com os participantes mantendo bancos de dados de propriedade de dinheiro vinculados a pseudônimos. Abrange a criação e transferência de dinheiro e a execução de contratos, incluindo mecanismos de arbitragem. O primeiro sozinho é considerado inviável por Wei Dai que usa o primeiro como base para criar o segundo protocolo

[6] Agem de forma descentralizada, buscando satisfazer as suas respectivas necessidades e do seu grupo, tal como defendido por Mises (2010, p.296) em que a ação, até mesmo despropositada, dos indivíduos é voltada à sua autossatisfação, isso inclui a parte dos ofertantes que desejam maximizar seu lucro. Sendo um fato que não necessita explicar as motivações dos agentes ou de seus respectivos valores morais.

2) A responsabilidade de registros e autenticação são de responsabilidade do que nomeia "servidores". Os indivíduos prosseguem com a verificação de mensagens enviadas para verificar a efetivação da criação, de transferências dos valores e o comprimento dos contratos. Para evitar fraudes e o conluio entre servidores Wei Dai (1993) propõem que os servidores deixem um valor tipo "caução" para garantir a sua idoneidade que caso burle o sistema terá seus valores retidos. Uma característica importante no sistema de Dai é a ideia de usar uma forma de *PoW* para validar as ações dos servidores, os indivíduos teriam que verificar apenas se aqueles que atuam como servidores agiram de forma idônea e registraram corretamente as transações. Os servidores seriam premiados de acordo com a quantidade de trabalho computacional feito.

2.2 O Desenvolvimento Técnico da Criptografia no uso do Bitcoin

A criptografia desempenha um papel fundamental na garantia da segurança e integridade das transações na blockchain. A tecnologia *blockchain,* tal como afirma Zhang et. al. (2020), tem se mostrado uma ferramenta versátil e disruptiva, encontrando aplicações significativas nos campos financeiro e econômico. Entre seus usos destacam-se a segurança de dados, os pagamentos internacionais, a liquidação de transações nos mercados financeiros, o financiamento comercial, a proteção contra ameaças cibernéticas, os seguros, a transferência de dinheiro em tempo real, o registro de propriedades, os acordos contratuais, a autenticação de identidades, os contratos e leilões inteligentes, além da detecção e prevenção de ataques.

No caso do Bitcoin, como explicam Antonopoulos e Wood (2019), é utilizada a função *hash* SHA-256, que converte dados em códigos alfanuméricos. Ou seja, *hash* é uma função que transforma uma frase qualquer em um código alfanumérico com 32 termos, 64 bits exatos, esse código de alfanumérico é formado quase aleatoriamente, de modo que não possa ser compreendido sua entrada pela sua saída. Essa transformação assegura que qualquer modificação na entrada gere um *hash* completamente distinto, reforçando a segurança do sistema. Existem dois modelos principais de criptografia: a simétrica e a assimétrica, que utilizam, respectivamente, chaves privadas e chaves públicas. No modelo de criptografia simétrica, uma única chave privada é empregada tanto para criptografar quanto para desencriptar as informações**.** Assim, a eficácia da criptografia simétrica depende da confidencialidade da chave, que não deve ser compartilhada com outros usuários. Essa abordagem, portanto, não é ideal para redes descentralizadas (MERKLE, 2019). No entanto, Nakamoto (2008) optou por um sistema de criptografia assimétrica, que utiliza pares de chaves: uma pública e uma privada. Merkle (2019) propõe o uso da função *hash* SHA-256, que transforma dados em códigos alfanuméricos com um comprimento fixo de 64 caracteres.

Essa característica assegura que qualquer pequena modificação na entrada resulte em um *hash* completamente diferente, facilitando a verificação da integridade das informações. Assim, a simples comparação das saídas *hash* permite verificar se as informações foram ou não alteradas. As chaves assimétricas utilizadas pelos usuários da rede *blockchain* operam por meio da curva elíptica[7] conhecida como *secp*256k1, um padrão criptográfico amplamente adotado nas criptomoedas, notadamente no protocolo do Bitcoin. O modelo de segurança baseado em criptografia de chave pública, como a curva elíptica *secp*256k1, elimina intermediários e fortalece a lógica descentralizada da rede, dificultando ataques como falsificação de identidade ou alteração retroativa das transações, sendo essa curva um dos pilares técnicos que sustentam a confiança distribuída no interior da *blockchain* (NARAYANAN et al., 2016; ANTONOPOULOS, 2017).

Tabela 1 - Elementos do Bloco de *blockchain*

Elemento	Descrição	Localização
Versão do bloco	Indica o protocolo utilizado na criação do bloco.	Cabeçalho
Hash do bloco anterior	Referência criptográfica ao bloco anterior, garantindo a integridade e a sequência da cadeia.	Cabeçalho
Raiz de *Merkle*	Hash resultante da combinação de todas as transações do bloco, permitindo verificação eficiente.	Cabeçalho
Timestamp	Registra a data e hora em que o bloco foi criado.	Cabeçalho
Target	Define o nível de dificuldade para mineração do bloco.	Cabeçalho
Nonce	Número aleatório ajustado pelos mineradores para encontrar um hash válido do bloco.	Cabeçalho
Transações	Conjunto de operações realizadas na rede, incluindo remetente, destinatário, valor e assinaturas digitais.	Corpo
Transação *Coinbase*	Primeira transação do bloco, que gera novas moedas e recompensa o minerador.	Corpo (início)

Elaboração Própria.

7 Curvas elípticas são equações algébricas do tipo $y^2 = x^3 + ax + b$, definidas sobre campos finitos — ou seja, conjuntos discretos de números inteiros modularmente restritos — sendo ideais para aplicações criptográficas devido à sua segurança e eficiência computacional (KOBLITZ, 1987; MILLER, 1986). Na prática da blockchain, como no protocolo Bitcoin, utiliza-se a curva secp256k1, que foi selecionada por sua estrutura matemática otimizada e ausência de elementos arbitrários que poderiam introduzir vulnerabilidades (NARAYANAN et al., 2016). O mecanismo de segurança baseia-se na adição de pontos e na chamada multiplicação escalar, onde um ponto público P, P da curva é multiplicado por um número inteiro secreto k, gerando o ponto Q. Embora P e Q sejam públicos, descobrir k é computacionalmente inviável, por ser um caso do problema do logaritmo discreto sobre curvas elípticas. Essa assimetria entre geração e reversão da chave é o que torna a criptografia de curva elíptica extremamente segura (FERGUSON; SCHNEIER; KOHNO, 2011), sustentando, assim, a integridade e a inviolabilidade das transações na blockchain.

A Tabela 1, demonstra como Nakamoto (2008) projetou os blocos como a estrutura fundamental para armazenar as informações que circulam na rede, dividindo-os em cabeçalho e corpo. É importante ressaltar que, Nakamoto (2008) combina o uso de chaves públicas e árvores de *Merkle,* para proporcionar uma estrutura segura e eficiente para as transações na *blockchain*. A chave pública atua como um pseudônimo único e inconfundível, garantindo a privacidade do usuário, que não precisa revelar sua identidade. Essa analogia pode ser feita com endereços de e-mail, que servem para identificar e facilitar a troca de informações.

Entretanto, é importante ressaltar que a chave pública não assegura anonimato absoluto. Ela é uma ferramenta de privacidade, como Ulrich (2015, p.15) observa: “as chaves não estão vinculadas à identidade de ninguém. Porém, se a identidade de uma pessoa estiver associada a uma chave pública, podemos rastrear todas as transações no blockchain relacionadas a essa chave.” Assim, se a identidade de um usuário estiver ligada a uma chave pública, é possível acessar todas as transações associadas, pois todas as informações relacionadas à chave pública ficam registradas de maneira pública e imutável na *blockchain*.

É inevitável que qualquer sistema de *blockchain*, caso permanecesse inalterado desde sua gênese, tornar-se-ia obsoleto diante do avanço tecnológico e das ameaças à segurança cibernética, comprometendo sua integridade estrutural e funcional. Ademais, a sobrevivência e relevância desses sistemas dependem diretamente de sua capacidade de adaptação, garantindo tanto a melhoria contínua das funcionalidades técnicas da rede quanto a sua resiliência diante das transformações tecnológicas e dos desafios emergentes. Para assegurar essa evolução, utiliza-se o mecanismo de "*fork*", Osório (2024) define como um processo que permite a implementação de atualizações na rede *blockchain*. A execução de um *fork* ocorre sob a premissa do consenso entre os participantes da rede, de modo que qualquer modificação significativa só se concretiza se houver adesão majoritária dos agentes envolvidos na *blockchain*.

Os *forks* podem ser classificados em duas categorias principais: os *soft forks* e os *hard forks*. No primeiro caso, as mudanças introduzidas na rede *blockchain* não alteram a sua estrutura fundamental, possibilitando compatibilidade entre o uso de diferentes versões do s*oftware* da *blockchain*. Em outras palavras, permite que a atualização seja implementada apenas para os nós que aceitarem a modificação, sem impedir a continuidade das transações por parte daqueles que permanecerem na versão anterior e como aponta Antonopulos (2017) – que uma *soft fork* é uma alteração nas regras de consenso que torna inválidos blocos anteriormente válidos. Como os nós antigos reconhecem os novos blocos como válidos, uma *soft fork* é compatível com versões anteriores. Essa abordagem possibilita que a adoção da atualização ocorra de forma gradual, à

medida que a rede avalia suas vantagens. Nesse modelo, todos os participantes da *blockchain* possuem poder de influência sobre a evolução da rede, sendo sua relevância proporcional à sua representatividade dentro do ecossistema. Mineradores exercem influência por meio de seu poder computacional, Exchange e serviços de carteiras digitais impactam o sistema pela quantidade de nós que operam, enquanto veículos de mídia especializados, influencers do setor e os próprios usuários finais desempenham um papel na legitimação ou rejeição de novas implementações.

Os *hard forks*, por outro lado, representam uma ruptura total com a estrutura anterior da rede, Antonopoulos (2017) explica que o *hard fork* como uma mudança nas regras de consenso que torna inválidos blocos anteriormente válidos ou vice-versa. Para que a rede se mantenha unida é necessário que os participantes atualizem para o novo software, contudo as divergências em relação atualização podem levar a uma separação dos participantes da rede *blockchain*, resultando na criação de uma nova rede *blockchain* que é independente da versão original. Esse processo de divisão é mais drástico que um *soft fork*, pois impossibilita a compatibilidade entre as redes, tornando inviável a transação direta entre os ativos das versões anteriores e posteriores. Assim, um *hard fork* frequentemente gera fragmentação entre os agentes do ecossistema, levando grupos distintos de usuários, desenvolvedores e mineradores a adotarem redes separadas, conforme seus interesses e alinhamentos tecnológicos. Esse tipo de atualização, embora mais disruptivo, pode ser necessário em momentos em que mudanças estruturais profundas sejam imprescindíveis para a evolução e segurança do sistema.

2.2.1 Criptomoedas

O Bitcoin e outras criptomoedas utilizam a tecnologia *blockchain* como base para oferecer um sistema financeiro descentralizado, seguro e resistente a interferências externas. Conforme Antonopoulos (2017) o caráter descentralizado do Bitcoin enfraquece as tentativas de controle e censura sobre usuários, destacando-o como uma alternativa robusta frente a políticas financeiras autoritárias, permitindo que indivíduos preservem e transfiram valor de forma independente, sem depender de intermediários ou de instituições centralizadas sujeitas a censura ou manipulação governamental.

Além de sua função como reserva de valor e proteção contra a inflação, o universo das criptomoedas se expandiu significativamente com redes como Ethereum e Solana. Essas redes vão além da simples transferência de ativos, servindo como ecossistemas amplamente versáteis que integram diferentes projetos e funcionalidades em suas infraestruturas. Uma das inovações mais relevantes nesse contexto é o uso de *smart contracts* (contratos inteligentes), que são programas

autoexecutáveis escritos diretamente na *blockchain*. Esses contratos permitem que transações e acordos ocorram automaticamente quando certas condições pré-estabelecidas são atendidas, eliminando a necessidade de intermediários e reduzindo custos e atrasos.

Com essa capacidade, redes como Ethereum e Solana não só abrem portas para soluções financeiras avançadas, mas também como defende Daily (2025) criam um ambiente propício para o desenvolvimento de aplicações descentralizadas (*dApps*). Isso inclui projetos relacionados a finanças descentralizadas (*DeFi*), jogos baseados em *blockchain, marketplaces* para *tokens* não fungíveis (*NFTs*), entre outros. Essas inovações transformam as redes *blockchain* em verdadeiros ecossistemas digitais, capazes de suportar e conectar diversos casos de uso, desde pagamentos até registros imutáveis e acordos digitais complexos.

Tabela 2 - Principais Criptomoedas

Criptomoeda	Símbolo	Preço (USD)	Market Cap (USD)	Volume 24h (USD)	Oferta Circulante
Bitcoin	BTC	$109 720,78	$2 180 884 660 083	$58 605 261 548	19 876 678 BTC
Ethereum	ETH	$2 704,44	$326 488 244 491	$22 834 600 713	120 722 643 ETH
BNB	BNB	$666,43	$93 891 686 366	$1 646 976 175	140 886 873 BNB
XRP	XRP	$2,31	$136 138 847 865	$2 923 930 906	58 819 652 442 XRP
Cardano	ADA	$0,7125	$25 187 805 960	$673 783 508	35 346 979 015 ADA
Solana	SOL	$160,02	$84 000 603 387	$3 759 084 679	524 925 217 SOL
Dogecoin	DOGE	$0,1949	$29 175 233 303	$1 215 680 599	149 621 346 384 DOGE

Fontes: *CoinMarketCap* (2025)

Na Tabela 2, encontram-se listadas as principais criptomoedas relevantes para o ecossistema da *blockchain*, com dados coletados no dia 1 de julho de 2025 a partir da plataforma *CoinMarketCap* (2025). A escolha desta data se justifica por critérios práticos, dado que se aproxima da finalização e entrega deste trabalho, permitindo a apresentação de informações mais recentes sobre o mercado de criptoativos. Cabe destacar que o objetivo central deste estudo não reside na análise quantitativa do comportamento de preços ou volume de mercado das criptomoedas, mas sim em apresentar o desenvolvimento das tecnologias associadas à *blockchain* e suas aplicações, sendo o mercado de criptomoedas um dos principais desdobramentos práticos dessa arquitetura. Portanto, os dados apresentados cumprem sua função instrumental, oferecendo um panorama atualizado que complementa a discussão teórica proposta neste subcapítulo, sem pretensão de esgotar o tema sob a ótica estatística ou financeira.

A seleção das criptomoedas consideradas na Tabela 2 – Bitcoin (BTC), Ethereum (ETH), BNB (BNB), XRP (XRP), Cardano (ADA), Solana (SOL) e Dogecoin (DOGE) – não se deu de forma

arbitrária, tampouco guiada apenas por critérios de capitalização de mercado ou popularidade momentânea. Trata-se de uma escolha fundamentada em sua relevância prática e tecnológica no contexto do desenvolvimento do ecossistema blockchain. O Bitcoin, como a primeira criptomoeda criada, permanece até hoje como a principal referência do setor, não apenas por sua primazia temporal, mas por representar de forma paradigmática a proposta de descentralização, escassez digital e soberania monetária. Em fevereiro de 2024, o Bitcoin voltou a ultrapassar o valor de mercado de 1 trilhão de dólares, impulsionado pela retomada do interesse institucional e pela aprovação dos ETFs de Bitcoin à vista nos Estados Unidos, o que reforça sua maturidade como ativo financeiro global e solidifica sua posição como reserva de valor no ambiente digital (FORBES, 2024).

No caso do Ethereum representa uma guinada tecnológica dentro do universo cripto, por ser a primeira rede blockchain a permitir a criação de contratos inteligentes (*smart contracts*), abrindo caminho para o surgimento de ecossistemas inteiros de aplicações descentralizadas *(dApps*), tokens não fungíveis (*NFTs*) e, sobretudo, das finanças descentralizadas (*DeFi*), revolucionando a lógica das interações econômicas digitais. Como formulado em seu *white paper*, o Ethereum foi concebido como uma "plataforma de próxima geração para contratos inteligentes e aplicações descentralizadas" (BUTERIN, 2014), ampliando significativamente o escopo funcional da blockchain para além da simples transferência de valores. Juntas, essas criptomoedas selecionadas não apenas ocupam posições de destaque nos rankings mundiais, como também representam diferentes camadas de inovação, funcionalidade e adoção que ajudam a compor um panorama abrangente das múltiplas frentes de desenvolvimento que conformam o universo *blockchain* contemporâneo.

O BNB (*token nativo da Binance*) foi escolhido por ilustrar o crescimento de soluções centralizadas dentro do universo cripto, além de representar um dos principais exemplos de *exchanges* que possuem *blockchains* próprias — no caso, a BNB Chain. O XRP, da Ripple, destaca-se por seu foco na integração com sistemas financeiros tradicionais e pela proposta de liquidez em transações transfronteiriças, mostrando como o *blockchain* pode dialogar com a infraestrutura bancária internacional. Cardano (ADA) e Solana (SOL) foram incluídas por serem projetos que buscam resolver os desafios técnicos enfrentados pelas primeiras gerações de *blockchain* — como escalabilidade, sustentabilidade e governança descentralizada — cada uma com arquiteturas inovadoras e visões distintas de desenvolvimento. Conforme destaca Schär (2021), essas plataformas representam uma nova geração de *blockchains* voltadas à superação das limitações estruturais das redes anteriores, promovendo soluções mais eficientes e adaptáveis às exigências crescentes do mercado.

Por fim, Dogecoin (DOGE), ainda que originada como uma criptomoeda de caráter humorístico, alcançou projeção significativa, tanto em volume de mercado quanto em adesão comunitária, sendo um exemplo paradigmático de como o valor atribuído a ativos digitais também está vinculado a fatores sociais, culturais e de marketing. Como aponta Catalini e Gans (2016), o valor de um criptoativo pode emergir não apenas de sua utilidade técnica, mas também da confiança coletiva, do engajamento social e da percepção de rede. Assim, essas criptomoedas foram escolhidas não apenas por sua capitalização de mercado, mas por representarem aspectos complementares e fundamentais da evolução tecnológica e econômica do ecossistema blockchain.

Assim, as criptomoedas evoluíram para muito mais do que simples instrumentos financeiros. Elas representam a vanguarda de uma revolução tecnológica que democratiza o acesso a serviços financeiros e inaugura novas possibilidades em economia digital, programação descentralizada e autonomia dos indivíduos sobre seus ativos e contratos.

3 DEBATE A RESPEITO DO IMPACTO DAS CRIPTOMOEDAS NO MUNDO CONTEMPORÂNEO

Desde a publicação do artigo “Bitcoin: A Peer-to-Peer Electronic Cash System”, por Satoshi Nakamoto (2008), o surgimento das criptomoedas tem provocado intensas discussões entre economistas, formuladores de políticas públicas e agentes do mercado financeiro. Inicialmente tratadas com ceticismo, as criptomoedas gradualmente conquistaram espaço na pauta econômica global ao desafiar estruturas tradicionais de emissão monetária, intermediação financeira e regulação estatal. Para Ferreira (2022, p. 22), os pilares que orientaram o surgimento das criptomoedas, pode ser definido a partir de três etapas: i) a primeira geração, liderada pelo Bitcoin, que estruturou a ideia de um “sistema de transações intricados e seguros”; ii) autonomia dos usuários e proteção de dados e iii) confiança no sistema criptográfico.

Nesse sentido, com uma capitalização de mercado que ultrapassa trilhões de dólares e crescente adesão por parte de investidores institucionais, governos e empresas, esses ativos digitais deixaram de ser um experimento marginal para se tornar um fenômeno econômico relevante. Assim sendo, é importante ressaltar posições diametralmente opostas a respeito dos impactos das criptomoedas no mundo contemporâneo, refletindo sobre o seu possível legado no longo prazo, a partir do debate existente entre economistas de diferentes vertentes teóricas.

3.1 Bitcoin, oferece uma resposta concreta ao dilema apresentado por Hayek

Com o avanço das tecnologias de blockchain e inteligência artificial, as moedas digitais estão aos poucos se tornando mais reconhecidas pelo público. O Bitcoin, como pioneiro nesse campo e a primeira criptomoeda a ser lançada, se destaca como a primeira moeda do mundo que permite transações anônimas de maneira descentralizada, utilizando a tecnologia *blockchain* e integrando conceitos de criptografia (LE TRAN; LEIRVIK, 2020). Nesse sentido, o Bitcoin e outras criptomoedas passam a utilizar a tecnologia *blockchain* como base para oferecer um sistema financeiro descentralizado, seguro e resistente a interferências externas. Conforme Antonopoulos (2017) o caráter descentralizado do Bitcoin enfraquece as tentativas de controle e censura sobre usuários, destacando-o como uma alternativa robusta frente a políticas financeiras autoritárias, permitindo que indivíduos preservem e transfiram valor de forma independente, sem depender de intermediários ou de instituições centralizadas sujeitas a censura ou manipulação governamental.

As primeiras aplicações práticas da tecnologia *blockchain,* como o Bitcoin criado por Nakamoto (2008), foram projetadas essencialmente para o setor financeiro, desafiando o modelo centralizado tradicional e introduzindo uma nova forma de organização das transações econômicas. A *blockchain* surge como uma tecnologia separativa ao inaugurar as chamadas finanças descentralizadas (*DeFi*), um paradigma que não apenas altera a estrutura operacional dos mercados financeiros, mas também reformula os incentivos e custos do sistema. Diferente do sistema financeiro convencional, baseado na intermediação bancária, gestão de risco e cooperação entre agentes para alcançar um equilíbrio de *Nash*[8] mutuamente benéfico. Em contrapartida a *blockchain* adota um modelo descentralizado onde a segurança e a confiabilidade derivam do consenso distribuído e da criptografia.

O modelo monetário vigente desde o colapso do sistema de *Bretton Woods* tem sido alvo de críticas severas, especialmente por pensadores da Escola Austríaca de Economia. Friedrich Hayek (1976), em suas obras, denunciava o monopólio estatal sobre a emissão monetária como um entrave à inovação no sistema financeiro e uma fonte de políticas inflacionárias que prejudicam a estabilidade econômica. Para Hayek (1976), a concentração desse poder nas mãos dos governos

[8] O conceito de equilíbrio de Nash, aplicado aos jogos cooperativos, estabelece que os agentes escolhem estratégias que maximizam o benefício coletivo, criando um estado em que nenhum participante possui incentivo para desviar unilateralmente, desde que os demais mantenham suas respectivas escolhas. Diferentemente dos jogos não cooperativos, nos quais cada indivíduo age de forma isolada visando sua própria maximização de utilidade, no contexto cooperativo considera-se não apenas a interação estratégica entre os jogadores, mas também a possibilidade de formação de coalizões e a subsequente distribuição dos ganhos resultantes dessa cooperação. A ideia central é que, uma vez estabelecido um equilíbrio dentro da coalizão, qualquer tentativa de um agente de alterar sua estratégia individualmente resultaria em uma situação menos vantajosa para ele próprio, reforçando a estabilidade da estrutura cooperativa e a previsibilidade dos resultados em um cenário de interdependência estratégica (NASH, 1951).

não apenas inibia o avanço tecnológico, mas também bloqueava a evolução natural do dinheiro como um instrumento criado e ajustado às necessidades dos indivíduos.

O economista austríaco foi além das críticas ao monopólio estatal e vislumbrou um sistema baseado em concorrência monetária. Inspirado pelo princípio de Vox populi, vox Dei (a voz do povo é a voz de Deus), o autor defendeu a criação de moedas privadas emitidas por empresas em competição direta. Esse modelo permitiria que o mercado elegesse, de forma natural e descentralizada, as moedas mais estáveis e úteis. A lógica, alinhada à visão de Ludwig von Mises sobre a "democracia de mercado", pressupunha que os consumidores abandonariam moedas inflacionárias ou instáveis, escolhendo aquelas que melhor atendessem suas necessidades. Nesse cenário, o mercado livre atuaria como um filtro, excluindo moedas inadequadas e incentivando a busca por estabilidade e confiança por parte dos emissores privados.

Contudo, Hayek reconhecia as dificuldades práticas de sua proposta, especialmente devido à resistência dos governos em renunciar ao monopólio sobre a moeda e dos benefícios decorrentes desse controle. Ele sugeriu que a transição para um sistema de moedas privadas poderia ocorrer de maneira gradual e silenciosa, inicialmente em nichos de mercado ou de forma marginal ao sistema monetário tradicional, até alcançar uma adoção ampla e inevitável. No entanto, Hayek deixou em aberto a questão de como, na prática, essa revolução poderia ser implementada, bem como os desafios associados à superação das barreiras impostas pelos Estados.

> [...] , a moeda fiduciária do banco central tende a incentivar o superendividamento, o que afeta a cultura de uma sociedade. Uma sociedade superendividada tenderá a ser mais materialista e orientada para o curto prazo. Em contraste, como observa Ammous (2018), um sistema monetário estável, como um padrão-ouro ou um sistema monetário baseado em uma criptomoeda com uma oferta inelástica, reduz a preferência social de tempo, ou seja, torna as pessoas mais orientadas para o futuro, promove a poupança e leva a um apogeu econômico, cultural e até artístico (BAGUS E LA HORRA; 2020, p. 425 – Tradução livre).

O advento da tecnologia *blockchain,* em especial o Bitcoin, ofereceu uma resposta concreta ao dilema apresentado por Hayek. Nakamoto (2008) concebeu um sistema de transações descentralizado, baseado em registros imutáveis e sustentado por uma rede de múltiplos agentes incentivados a cooperar de maneira voluntária. A inovação trouxe a possibilidade de uma moeda global, livre de intermediários centralizados, que não depende da confiança em autoridades ou governos. O Bitcoin materializou a visão de uma moeda privada e autônoma, permitindo que as pessoas transacionem de forma segura e transparente, enquanto preservam sua liberdade econômica. Nesse sentido, a blockchain representa não apenas um avanço tecnológico, mas

também a concretização de uma ideia visionária, sendo o elo perdido que faltava para viabilizar o sistema competitivo e descentralizado que Hayek idealizou.

3.2 Criptomoedas: inovação ou ameaça ao sistema monetário tradicional?

Mattos, Abouchedid, Araújo e Silva (2020) tecem uma análise por meio de uma visão pós-keynesiana, afirmando que o Bitcoin não terá sucesso em comparação às moedas fiduciárias devido ao seu alto poder especulativo e, com isso, altamente volátil o que o enfraquece em uma economia capitalista. Esses mesmos autores, trazem para o debate, o papel das criptomoedas estatais.

Já economistas ligados a instituições financeiras internacionais e bancos centrais tendem a ver as criptomoedas com maior desconfiança. Aglietta (2018, p.198), faz uma ressalva quanto ao papel dos ativos financeiros em seu estudo sobre "Finance and Macroeconomics: The Preponderance of the Financial Cycle":

> Os mercados de ativos são sobre o futuro. São mercados que transmitem trocas de promessas e compromissos que geralmente são contratuais. O futuro é o tempo das expectativas e, portanto, das crenças sobre o futuro. Os mercados financeiros são, portanto, uma organização por meio da qual as crenças individuais sobre o futuro interagem para dar origem a uma crença coletiva. Por meio da mediação dos mercados financeiros, as crenças sobre o futuro influenciam as ações atuais dos participantes do mercado. (Tradução livre)

Filippi (2014), levanta a questão da "natureza intrínseca das criptomoedas" ao estudar o Bitcoin. O autor, levanta a questão da evasão fiscal, já que ela não é rastreável, logo concluí que é necessário algum nível de regulamentação, mas que ela não seja "sufoque a inovação nesse ecossistema nascente".

Paul Krugman (2018) argumenta que o Bitcoin não cumpre adequadamente as três funções clássicas da moeda – unidade de conta, meio de troca e reserva de valor – e que sua volatilidade o torna inadequado como substituto do dinheiro fiduciário. O economista nova-iorquino ironizou o entusiasmo em torno do Bitcoin ao classificá-lo como "uma bolha com aspirações anarquistas", revelando, nesse diagnóstico, uma cosmovisão (*Weltanschauung*) que privilegia modelos de organização social baseados em autoridade central e intervenção estatal, em nítido contraste com os princípios fundadores do ecossistema *blockchain,* cuja estrutura repousa na descentralização, no consenso distribuído e na eliminação de intermediários.

Nessa direção, Barros (2017, p. 8) "conclui-se [...] a não considerar que o Bitcoin (ou as criptomoedas) se enquadra na definição usual do que se entende por moeda, por não atender as

prerrogativas de aplicabilidade dos mercados externos ao meio virtual". Nesse mesmo caminho, Ulrich (2014) ressalta que o Bitcoin pode ser considerado um "meio de troca secundário" ou uma espécie de quase-moeda, isso devido ele não ser considerado dinheiro e nem um meio de "troca universal".

Sobre o tema, "criptomoedas estatais", é importante ressaltar que no debate econômico no que diz respeito à natureza das criptomoedas enquanto substitutas ou complementares ao dinheiro estatal, destaca-se o pensamento de Friedrich Hayek (1976). Para economistas alinhados ao pensamento austríaco, o surgimento de moedas privadas e descentralizadas é desejável, pois rompe com o monopólio estatal da moeda, permitindo que a moeda volte a evoluir suas tecnologias e funcionamento pelo teste de mercado em que são os indivíduos como consumidores que assumirão sua preferência pelo meio monetário mais eficaz. Sob essa ótica, criptomoedas como o Bitcoin representam um avanço rumo à liberdade monetária e à soberania individual.

Baur et. al. (2018) analisaram como o Bitcoin é usado atualmente e qual uso deve prevalecer no futuro. A principal conclusão do estudo, foi que o Bitcoin não tem uma relação forte com os ativos tradicionais, sendo mais utilizado como uma forma de investimento especulativo do que como uma moeda ou meio de troca alternativo.

Lin et. al. (2025), ressaltam que a partir de um estudo empírico que o índice de preços dos insumos afeta de maneira substancial e desfavorável o desempenho do Bitcoin. Além disso, a variação da cotação do dólar americano influencia negativamente os retornos dessa criptomoeda, enquanto os rendimentos dos títulos do Tesouro exercem uma influência benéfica.

No entanto, para uma corrente crítica[9], o sistema financeiro baseado em criptomoedas carece de respaldo institucional suficiente para assegurar estabilidade macroeconômica, sendo frequentemente destacados como riscos a volatilidade extrema dos ativos digitais, a ausência de garantias patrimoniais, a dificuldade de regulação e a possibilidade de uso em atividades ilícitas. Tais críticas, embora relevantes, muitas vezes ignoram os avanços tecnológicos e os mecanismos próprios de autorregulação presentes nas finanças descentralizadas (DeFi), preferindo reafirmar modelos tradicionais de política monetária e controle centralizado.

O ceticismo institucional, nesse sentido, reflete não apenas preocupações técnicas, mas também uma resistência ideológica à lógica de um sistema autorregulado – próprio das redes blockchain – que subverte as formas clássicas de controle e intervenção governamental. Nesse sentido vale destacar, algumas críticas que estão fincadas em pilares, que merecem ser destacados, pois ao

[9] Segundo o Fundo Monetário Internacional (2021), a ausência de padrões regulatórios internacionais para criptoativos pode gerar riscos sistêmicos, incentivando a arbitragem regulatória e comprometendo a estabilidade financeira global, o que reforça a necessidade de uma regulação ampla, coerente e coordenada entre os países.

rejeitarem a legitimidade das criptomoedas como uma nova camada do sistema financeiro global, seus opositores reafirmam uma visão de mundo que enxerga a ordem econômica como dependente do poder coercitivo do Estado, em oposição à confiança algorítmica e à coordenação espontânea que caracterizam as redes descentralizadas. Tal rejeição, mais do que um juízo técnico, revela uma tensão filosófica sobre os fundamentos da confiança, da autoridade e da liberdade no mundo contemporâneo.

Outro ponto central do debate gira em torno da regulação. O crescimento acelerado das criptomoedas levanta preocupações quanto à evasão fiscal, transações fora do arcabouço jurídico e penal das nações e à possível instabilidade dos mercados financeiros globais. Economistas mais alinhados à ortodoxia monetária, como Rogoff (2019, p.87), defendem a necessidade de um arcabouço regulatório internacional robusto, capaz de disciplinar o uso desses ativos e mitigar riscos sistêmicos. Sinaliza que embora a tecnologia blockchain seja reconhecidamente promissora, sua aplicação em criptomoedas com elevado grau de anonimato e descentralização é, em última instância, politicamente insustentável, afirmando que "a história mostra que o Estado sempre acabará por intervir fortemente na gestão da moeda", sinalizando que o futuro dessas tecnologias dependerá menos da inovação técnica e mais da disposição dos governos em regulamentá-las ou incorporá-las aos sistemas monetários já existentes. Nesse contexto, prevê-se que o legado mais duradouro das criptomoedas não será a substituição do dinheiro estatal por ativos descentralizados como o Bitcoin, mas sim a digitalização das moedas fiduciárias por meio das chamadas Moedas Digitais de Banco Central (CBDCs)[10], que manteriam o controle monetário nas mãos das autoridades nacionais. Essa perspectiva vinga os estatistas, reforçando a crença em uma ordem necessariamente centralizada e dependente das instituições estatais para o funcionamento do sistema financeiro.

Em contrapartida, pensadores mais ligados à inovação tecnológica advertem sobre os perigos de uma regulação excessiva. Vitalik Buterin (2014), criador do Ethereum, argumenta que políticas públicas demasiadamente restritivas podem sufocar o potencial disruptivo do ecossistema blockchain, comprometendo o desenvolvimento de soluções descentralizadas nas áreas de finanças (*DeFi*), contratos inteligentes, identidade digital e governança algorítmica. A colaboração prudente

[10] O Drex representa a implementação brasileira da chamada Central Bank Digital Currency (CBDC), ou moeda digital de banco central. Trata-se de uma extensão digital do real, emitida e garantida pelo Banco Central do Brasil, que busca combinar a estabilidade institucional da moeda fiduciária com a eficiência e rastreabilidade das tecnologias de registro distribuído. O projeto insere o país em um movimento global de digitalização das moedas soberanas, sinalizando uma tentativa de preservar a relevância da política monetária frente ao avanço dos criptoativos e sistemas de pagamento descentralizados. Cf. BANCO CENTRAL DO BRASIL. A moeda digital oficial brasileira (Drex) – Referências básicas. Brasília, nov. 2023.

entre Estado e mercado, portanto, torna-se indispensável para evitar tanto o colapso da inovação quanto o advento de zonas de desordem financeira.

Bouri et.al. (2020), concluem que usar criptomoedas para proteger ações traz benefícios. Mais especificamente, os resultados indicam que os portfólios protegidos com criptomoedas oferecem uma diversificação melhor do que aqueles que têm apenas ações, o que pode ajudar a reduzir riscos e melhorar o desempenho.

Em defesa ética das criptomoedas, Bagus e La Horra (2020, p. 423), concluíram que:

> [...], se as criptomoedas se tornassem um meio de troca generalizado, a capacidade dos governos de realizar políticas monetárias, fiscais e de drogas seria prejudicada. Argumentamos que esse seria um resultado eticamente desejável tanto do ponto de vista dos direitos de propriedade privada quanto do utilitarismo, uma vez que forçaria os governos a reduzir seu tamanho e escopo nessas três áreas. (Tradução livre)

A disputa entre inovação e controle estatal é, assim, uma das tensões fundamentais do debate contemporâneo sobre criptomoedas. De um lado, a promessa de uma infraestrutura descentralizada capaz de ampliar a liberdade econômica e a eficiência das transações. De outro, a necessidade de preservar a ordem jurídica, a estabilidade macroeconômica e a soberania monetária. O equilíbrio entre essas forças será determinante para definir não apenas o futuro das criptomoedas, mas também os contornos do sistema financeiro global nas próximas décadas.

Independentemente do destino das criptomoedas enquanto ativos específicos, seu legado institucional já é visível. A arquitetura descentralizada do blockchain, a transparência algorítmica das transações e o conceito de auto-custódia promovem um novo paradigma de confiança e registro, que desafia a intermediação tradicional em setores como finanças, logística, identidade digital e até mesmo a governança política. Destarte, o impacto das criptomoedas vai além da moeda. Elas representam a consolidação de uma mentalidade descentralizadora, que tende a inspirar reformas em diferentes áreas da sociedade. Para economistas atentos às transformações institucionais de longo prazo, o blockchain pode servir como uma ferramenta eficaz para garantir direitos de propriedade, promover a formalização de ativos e integrar populações à economia formal, especialmente em países em desenvolvimento (DE SOTO, 2017).

4 À GUISA DE CONCLUSÃO

A tecnologia *blockchain* surge como um divisor de águas no contexto da economia digital, redesenhando os contornos do sistema financeiro e desafiando estruturas tradicionais centralizadoras. Seu potencial ultrapassa a mera transferência de valor, estendendo-se à segurança cibernética, contratos inteligentes, rastreabilidade em cadeias produtivas e à formação de

ecossistemas descentralizados robustos. A evolução dessa tecnologia, por meio de mecanismos como *forks*, demonstra sua capacidade de adaptação frente às exigências de um mundo em constante mutação. Contudo, seu avanço não ocorre sem resistência: o embate entre visões políticas antagônicas — entre a liberdade individual proporcionada pela descentralização e o ímpeto de controle estatal — revela uma tensão essencial no debate sobre o futuro das finanças. Enquanto alguns países apostam na inovação regulatória para fomentar um ambiente propício ao desenvolvimento da *blockchain*, outros optam pela repressão tecnológica como forma de preservar o status quo.

A regulamentação, embora necessária para mitigar riscos sistêmicos e promover um ambiente minimamente seguro para inovação, não pode converter-se em um instrumento de sufocamento da liberdade econômica, tampouco em uma barreira à autonomia dos indivíduos. Tal linha tênue entre proteção legítima e controle abusivo exige vigilância intelectual e cívica constante. Cabe, portanto, à sociedade civil, aos formuladores de políticas públicas e aos agentes de mercado discernirem entre o zelo honesto e o autoritarismo disfarçado de prudência técnica. O uso do termo prudência, nesse contexto, deve resgatar seu sentido clássico, conforme delineado pela tradição aristotélica, como uma virtude que orienta a ação reta diante da complexidade. Não por acaso, Edmund Burke (1968, p. 148), estadista britânico e defensor de uma ordem política ancorada na razão prática, afirmou: “A prudência é não apenas o primeiro dos deveres em tempos difíceis, mas também a primeira das virtudes políticas; e uma prudência de longo alcance e bem fundamentada é a melhor garantia contra os abusos do poder, tanto revolucionário quanto tirânico.” Nesse sentido, uma regulamentação eficaz deve se estruturar não em torno do medo ou da ânsia de controle, mas na prudência que salvaguarda a liberdade, sustenta a inovação e protege os cidadãos contra os abusos que podem emergir tanto do mercado quanto do Estado.

O futuro da *blockchain* dependerá da forma como esses vetores forem equilibrados: se será consolidada como instrumento de emancipação e inovação, ou se será domesticada pelo medo e pela burocracia. A criação da *blockchain* inaugura uma nova maneira descentralizada de tratar o uso da informação — incluindo as finanças — o que viabiliza a criação e ampliação de múltiplos setores de empreendimentos. Nesse contexto, as finanças descentralizadas (*DeFi*) já se constituem como um segmento relevante dentro do universo financeiro, assumindo papel cada vez mais presente no cotidiano de profissionais da área e influenciando de forma concreta a gestão das finanças pessoais. Diante disso, mostra-se sábio e necessário fomentar novas pesquisas que aprofundem a compreensão técnica do ecossistema *blockchain*, examinem suas interações com eventos macroeconômicos e investiguem suas possíveis correlações com o mercado financeiro tradicional.

O debate entre economistas sobre as criptomoedas revela profundas divergências de cosmovisão quanto ao papel do Estado, à natureza da moeda e à relação entre tecnologia e instituições. Para os mais estatistas as criptomoedas são uma utopia liberal e tecnocrática fadada ao colapso; para os defensores da liberdade e da inovação, são a semente de uma nova ordem monetária mais livre, eficiente e democrática.

Independentemente do julgamento de valor, é inegável que as criptomoedas e o ecossistema blockchain já impactam o mundo contemporâneo. Seu legado será definido pela capacidade de equilibrar inovação com estabilidade, liberdade com responsabilidade e descentralização com governança eficaz. Cabe aos economistas compreender esse fenômeno em sua complexidade. Nas palavras de Hayek, trata-se de um "fenômeno complexo" — que emerge da interação entre múltiplos indivíduos em um processo de mercado, e que não pode ser compreendido a partir da lógica de uma ordem simples, onde uma razão central planejadora seria capaz de organizar o microcosmo das interações humanas (HAYEK, 1973). Assim, o advento do ecossistema blockchain deve ser entendido como um fenômeno de mercado, com todas as implicações que esse tipo de dinâmica carrega.

Portanto, impressões apocalípticas ou visões utópicas de uma nova era de paraíso tecnológico não condizem com a arquitetura do *blockchain*. Trata-se de um sistema ancorado na experiência prática, cujo avanço se dá por meio da evolução e do aprimoramento constante de suas tecnologias, como se observa nos *Forks* e nos ciclos de mercado. O consenso distribuído da rede permite que os indivíduos aprendam, ajustem rumos e se aproximem da realidade desejada. Ao economista, como estudioso dos fenômenos de mercado, cabe observar com razão e diligência, evitando tanto o entusiasmo acrítico quanto o ceticismo dogmático.

REFERÊNCIAS

AGLIETTA, M. Finance and Macroeconomics: The Preponderance of the Financial Cycle. **Revue de l'OFCE** . N° 157, p. 197-224, 2018/3. Disponível em: https://shs.cairn.info/revue-de-l-ofce-2018-3-page-197?lang=en. Acesso em: 23 de maio de 2025.

ANTONOPOULOS, Andreas M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2. ed. Sebastopol: O'Reilly Media, 2017.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. 2. ed. Birmingham: Packt Publishing, 2019.

BAGUS, Philipp; LA HORRA, Luis P. An ethical defense of cryptocurrencies. **Business Ethics**, Env & Resp. p. 423–431, 2021:30. Disponível em: https://onlinelibrary.wiley.com/doi/epdf/10.1111/beer.12344. Acesso em 25 de maio de 2025.

BANCO CENTRAL DO BRASIL. A moeda digital oficial brasileira (Drex) – Referências básicas. Brasília, nov. 2023. Disponível em: https://www.bcb.gov.br/content/estabilidadefinanceira/real_digital_docs/drex_referencias_basicas_nov2023.pdf. Acesso em: 1 abr. 2025.

BARROS, Dákini M. Moeda e Criptomoeda: Uma análise do Bitcoin sobre a perspectiva pós-keynesiana. Monografia submetida ao curso de Ciências Econômicas da Universidade Federal de Santa Catarina, 2017.

BAUR, D. G., HONG, K., & LEE, A. D. Bitcoin: Medium of exchange or speculative assets? Journal of International Financial Markets, Institutions and Money, Volume 54, p.177–189, 2018. https://doi.org/10.1016/j. intfin.2017.12.004

BOURI, Elie; LUCEY, Brian; ROUBAUD, David. Cryptocurrencies and the downside risk in equity Investments. Finance Research Letters, Volume 33, March 2020, 101211. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1544612318306342. Acesso em: 26 de maio de 2025.
BOVÉRIO, Maria Aparecida; DA SILVA, Victor Ayres Francisco. Blockchain: uma tecnologia além da criptomoeda virtual. *Revista Interface Tecnológica*, v. 15, n. 1, p. 109-121, 2018.

BURKE, Edmund. Reflections on the Revolution in France. Edited by Conor Cruise O'Brien. London: Penguin Books, 1968. (Penguin Classics).

BUTERIN, V. A Next-Generation Smart Contract and Decentralized Application Platform. Ethereum White Paper, 2014.

CATALINI, Christian; GANS, Joshua S. Some Simple Economics of the Blockchain. MIT Sloan Research Paper, n. 5191-16, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598. Acesso em: 16 abr. 2025.

COINMARKETCAP. Criptomoedas: capitalização de mercado, volume e preços. 2025. Disponível em: https://coinmarketcap.com/. Acesso em: 01 jun. 2025.

COPPERBERG. Building resilient supply chains: how blockchain drives efficiency and trust. Disponível em: https://www.copperberg.com/building-resilient-supply-chains/. Acesso em: 2 abr. 2025.

DAI, Wei. b-money. [S.l.: s.n.], 1998. Disponível em: https://bitcoinstan.io/prehistory/doc/1998_3.pdf. Acesso em: 10 jun. 2025.

DEMIRKAN, Sebahattin; DEMIRKAN, Irem; MCKEE, Andrew. Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, v. 7, n. 2, p. 189-208, 2020.

DE FILIPPI, P.; WRIGHT, A. Blockchain and the law: the rule of code. Cambridge: Harvard University Press, 2018.

DE SENNA, Viviane; SOUZA, Adriano M. Criptomoedas e Sistema Financeiro: Revisão Sistemática de Literatura. **RAE-Revista de Administração de Empresas**, FGV EAESP. V. 63, n. 4 , 2023, p. 1-22 .

DE SOTO, Hernando. The Potential of Blockchain to Transform Developing Economies. World Economic Forum, 2017. Disponível em: https://www.weforum.org/agenda/2017/06/blockchain-has-the-potential-to-transform-developing-economies/. Acesso em: 10 maio 2025.

FMI – FUNDO MONETÁRIO INTERNACIONAL. A regulação global dos criptoativos deve ser ampla, coerente e coordenada. Publicado em 9 dez. 2021. Disponível em: https://www.imf.org/pt/Blogs/Articles/2021/12/09/blog120921-global-crypto-regulation-should-be-comprehensive-consistent-coordinated. Acesso em: 10 maio 2025

FERGUSON, N.; SCHNEIER, B.; KOHNO, T. Criptografia prática. 2. ed. Rio de Janeiro: Alta Books, 2011.

FERREIRA, Juliana W. V. O Futuro do Dinheiro: O papel das Criptomoedas na evolução da moeda fiduciária. Monografia Jurídica apresentada ao Curso de Direito do Instituto de Ciências Humanas e Sociais de Volta Redonda, pertencente à Universidade Federal Fluminense, 2022.

FILIPPI, P. D. Bitcoin: A regulatory nightmare to a libertarian dream. ***Internet Policy Review***, *3*(2), p. 1–43, 2014. Disponível em : https://doi.org/10.14763/. Acesso em:26 de maio de 2025.
FORTUNA ,J.; HOLTZ, B., NEFF, J. Evolutionary Structural Analysis of the Bitcoin Network. 2013. Disponível em: https://pdfs.semanticscholar.org/35b2/cac7bb85b6051f80b9eacfe292435c84a5c0.pdf. Acesso em: 23 de maio de 2025.
GERVAIS, Arthur et al. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. p. 3-16.

GURTU, Amulya; JOHNY, Jestin. Potential of blockchain technology in supply chain management: a literature review. International Journal of Physical Distribution & Logistics Management, v. 49, n. 9, p. 881-900, 2019.

HAYEK, Friedrich August von. Law, legislation and liberty: a new statement of the liberal principles of justice and political economy. Vol. 1: Rules and order. Chicago: University of Chicago Press, 1973.

HAYEK, Friedrich August von. A desnacionalização da moeda: o argumento refinado. 2. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2012. Traduzido de: The denationalization of money. Publicado originalmente em 1976.

HAYEK, Friedrich August. Denationalisation of money: an analysis of the theory and practice of concurrent currencies. Ludwig von Mises Institute, 1976.

KOBLITZ, N. Elliptic curve cryptosystems. Mathematics of Computation, v. 48, n. 177, p. 203–209, 1987.

KRUGMAN, Paul. Bubble, bubble, fraud and trouble. The New York Times, 29 jan. 2018. Disponível em: https://www.nytimes.com/2018/01/29/opinion/bitcoin-bubble-fraud.html. Acesso em: 06 maio 2025.

LE TRAN, Vu; LEIRVIK, Thomas. Efficiency in the markets of crypto-currencies. **Finance Research Letters,** Volume 35, 101382, 2020. Disponível em: https://www.sciencedirect.com/science/article/pii/S1544612319310438. Acesso em 24 de maio 2025.

LIANG, J., LI, L., & ZENG, D. Evolutionary dynamics of cryptocurrency transaction networks: An empirical study. PLOS ONE, 13(8), 2018. e0202202. https://doi.org/10.1371/journal.pone.0202202

LIN, Minghui; LIU, Ye; SHENG, Vincent Ng K. Analysis of the impact of macroeconomic factors on cryptocurrency returns - Based on quantile regression study. **International Review of Economics and Finance**, Volume 97, 103757, 2025 Disponível em: https://www.sciencedirect.com/science/article/pii/S1059056024007494. Acesso em 24 de maio de 2025.

LONDON DAILY. Ethereum vs. Solana: Which blockchain is better? London Daily News, 2025. Disponível em: https://www.londondaily.news/ethereum-vs-solana-which-blockchain-is-better/. Acesso em: 2 abr. 2025.

MATTOS, Olívia B.; ABOUCHEDID, Saulo; ARAÚJO E SILVA, Laís. As criptomoedas e os novos desafios ao sistema monetário: uma abordagem pós-keynesiana. **Economia e Sociedade**, Campinas, v. 29, n. 3 (70), p. 761-778, 2020.

MERKLE, Ralph C. Protocols for public key cryptosystems. In: Secure communications and asymmetric cryptosystems. Routledge, 2019. p. 73-104.

MILLER, V. Use of elliptic curves in cryptography. In: Advances in Cryptology—CRYPTO'85 Proceedings. Springer, 1986. p. 417–426.

MISES, Ludwig von. Ação humana: um tratado de economia. São Paulo: Instituto Ludwig von Mises Brasil, v. 1949, 2010.

MOUGAYAR, William; BUTERIN, Vitalik. The Business Blockchain: Promise, Practice, and the Application of the Next Internet Technology. Hoboken: Wiley, 2016.

NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. Satoshi Nakamoto, 2008.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press, 2016.

NASH, John. Non-cooperative games. Annals of Mathematics, Princeton, v. 54, n. 2, p. 286-295, 1951. Disponível em: https://www.jstor.org/stable/1969529. Acesso em: [data de acesso].

NASIR, R. Criptomoedas e o controle governamental: uma análise das restrições à adoção e uso de carteiras descentralizadas. São Paulo: Editora Cripto, 2023.

OLIVEIRA, L. et al. To token or not to token: Tools for understanding blockchain tokens. ICIS, , 2018. Disponível em:

https://www.zora.uzh.ch/id/eprint/157908/1/To%20Token%20or%20not%20to%20Token_%20Tools%20for%20Understanding%20Blockchain%20Toke.pdf

OSÓRIO JR, E. Consenso no Bitcoin: Como a Rede Evolui sem Comprometer a Segurança. Disponível em: <https://www.eddieoz.com/consenso-no-bitcoin-como-a-rede-evolui-sem-comprometer-a-seguranca/#:~:text=No%20processo%20de%20consenso%2C%20mudan%C3%A7as,mudan%C3%A7as%20compat%C3%ADveis%20com%20vers%C3%B5es%20anteriores.>. Acesso em: 16 mar. 2025.

PRINS, Nomi. Permanent Distortion: How the Financial Markets Abandoned the Real Economy Forever. New York: PublicAffairs, 2022

ROGOFF, Kenneth. O fim do dinheiro e o futuro da civilização financeira. São Paulo: Portfolio-Penguin, 2019.

ROTHBARD, M. N. O que o governo fez com o nosso dinheiro? 3. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2012. (Original de 1990).

SCHÄR, Fabian. Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. Federal Reserve Bank of St. Louis Review, v. 103, n. 2, p. 153–174, 2021. Disponível em: https://research.stlouisfed.org/publications/review/2021/02/05/decentralized-finance-on-blockchain-and-smart-contract-based-financial-markets. Acesso em: 16 abr. 2025.

SWAN, Melanie. *Blockchain: Blueprint for a New Economy*. Sebastopol, California: O'Reilly Media Inc., 2015. 149 p.

TAYLOR, Paul J. et al. A systematic literature review of blockchain cyber security. Digital Communications and Networks, v. 6, n. 2, p. 147-156, 2020. ULRICH, Fernando. Bitcoin-a moeda na era digital. Journal, volume, v. 2, p. 239, 1892.

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

ZHANG, Li et al. The challenges and countermeasures of blockchain in finance and economics.

Systems Research and Behavioral Science, v. 37, n. 4, p. 691-698, 2020.

José Alves de Melo Júnior

Bitcoin: Tecnologias subjacentes e um debate acerca da função das criptomoedas na sociedade contemporânea

Trabalho de Conclusão de Curso (TCC) apresentado à Coordenação do Curso de Ciências Econômicas do Campus Agreste da Universidade Federal de Pernambuco – UFPE, como requisito parcial para a obtenção do grau de bacharel em Ciências Econômicas.

Aprovado em: 21/07/2025.

BANCA EXAMINADORA

Prof.ª Dr.ª Lucilena Ferraz Castanheira Corrêa
(Orientadora)
Núcleo de Gestão
Universidade Federal de Pernambuco

Prof.ª Dr.ª Isabella Leitão Neves Frota
Núcleo de Gestão
Universidade Federal de Pernambuco

Profº.Dr.º Klebson Humberto de Lucena Moura
Núcleo de Gestão
Universidade Federal de Pernambuco