UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE ECONOMIA
CIÊNCIAS ECONÔMICAS

LÁZARO DE JESUS RABELO

CRIPTOMOEDAS NO BRASIL:
DESAFIOS E PERSPECTIVAS PARA A ADOÇÃO NO COTIDIANO

JUIZ DE FORA
2024

LÁZARO DE JESUS RABELO

CRIPTOMOEDAS NO BRASIL:

DESAFIOS E PERSPECTIVAS PARA A ADOÇÃO NO COTIDIANO

Monografia apresentada a Faculdade de Economia da Universidade Federal de Juiz de Fora, como requisito à obtenção do título de bacharel em Ciências Econômicas.

Orientador: Prof. Alexandre Zanini

JUIZ DE FORA

2024

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Rabelo, Lázaro de Jesus.
Criptomoedas no Brasil : Desafios e Perspectivas Para a Adoção no Cotidiano / Lázaro de Jesus Rabelo. -- 2024.
55 f. : il.

Orientador: Alexandre Zanini
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Juiz de Fora, Faculdade de Economia, 2024.

1. Criptomoedas. 2. Blockchain. 3. Sistemas Monetários. 4. Mercado Financeiro. 5. Evolução Financeira. I. Zanini, Alexandre, orient. II. Título.

UNIVERSIDADE FEDERAL DE JUIZ DE FORA
REITORIA - FACECON - Depto. de Economia

FACULDADE DE ECONOMIA / UFJF

ATA DE APROVAÇÃO DE MONOGRAFIA II (MONO B)

Na data de 02/07/2024, a Banca Examinadora, composta pelos professores

1 – Alexandre Zanini - orientador; e

2 – Eduardo Gonçalves,

reuniu-se para avaliar a monografia do acadêmico **LÁZARO DE JESUS RABELO**, intitulada: **CRIPTOMOEDAS NO BRASIL: DESAFIOS E PERSPECTIVAS PARA A ADOÇÃO NO COTIDIANO**.

Após primeira avaliação, resolveu a Banca sugerir alterações ao texto apresentado, conforme relatório sintetizado pelo orientador. A Banca, delegando ao orientador a observância das alterações propostas, resolveu **APROVAR** a referida monografia.

ASSINATURA ELETRÔNICA DOS PROFESSORES AVALIADORES

Documento assinado eletronicamente por **Alexandre Zanini**, **Professor(a)**, em 02/07/2024, às 18:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Eduardo Goncalves**, **Professor(a)**, em 03/07/2024, às 16:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no Portal do SEI-Ufjf (www2.ufjf.br/SEI) através do ícone Conferência de Documentos, informando o código verificador **1846085** e o código CRC **7072B41E**.

Referência: Processo nº 23071.919191/2024-22 SEI nº 1846085

AGRADECIMENTOS

Gostaria de expressar minha profunda gratidão a todos que me acompanharam ao longo dos anos de graduação, tornando possível a rica experiência de estudar Economia na Universidade Federal de Juiz de Fora.

Agradeço à minha mãe, cuja criação e educação foram fundamentais para meu desenvolvimento. Também sou grato à minha noiva, cujo apoio incondicional e incentivo estiveram presentes em todos os momentos.

Agradeço a todos os meus professores que pavimentaram o caminho para que eu chegasse até aqui. Em especial, quero mencionar os professores do curso de Economia da UFJF. Por fim, expresso minha gratidão ao professor Alexandre Zanini, que aceitou ser meu orientador, contribuindo significativamente para o meu percurso acadêmico.

LISTA DE FIGURAS

LISTA DE SIGLAS

ACM	Association for Computing Machinery
ATM	Automatic Teller Machine
BDTD	Biblioteca Digital de Teses e Dissertações
CAGR	Taxa de crescimento anual composta.
CEPAL	Comissão Econômica para a América Latina e o Caribe
CNC	Confederação Nacional do Comércio de Bens, Serviços e Turismo
CONSUAS	Conselho Nacional de Economia Solidária
dApps	Decentralized Applications
DDoS	Ataque de Negação de Serviço Distribuído
DeFi	Decentralized Finance
DLT	Distributed Ledger Technology
IBGE	Instituto Brasileiro de Geografia e Estatística
IEEE	Institute of Electrical and Electronics Engineers
ILO	International Labour Organization
IoT	Internet of Thing
MEC	Ministério da Educação
MTE	Ministério do Trabalho e Emprego
OIT	Organização Internacional do Trabalho
P2P	Peer-to-Peer
PDA	Programa de Desenvolvimento Associativo
PoS	Prova de Participação
SCiELO	Scientific Electronic Library Online

RESUMO

O objetivo desta pesquisa é investigar os desafios e perspectivas para a adoção das criptomoedas no cotidiano. A análise foca em identificar os benefícios potenciais, usos práticos e os obstáculos técnicos, regulatórios, de segurança, educacionais e de infraestrutura que influenciam a aceitação e a integração generalizada das criptomoedas. Utilizou-se uma metodologia de revisão bibliográfica narrativa, abrangendo uma ampla gama de literatura sobre criptomoedas, blockchain, tecnologia financeira, segurança digital, regulamentação e educação financeira. A pesquisa baseou-se em plataformas como BDTD, SCiELO, Periódicos, IEEE, ACM, além de dados de fontes online como Statista e Banco Mundial. Os resultados indicam que as criptomoedas possuem um potencial significativo para transformar a economia global e o cotidiano das pessoas. Elas têm sido utilizadas em uma variedade de aplicações práticas, incluindo pagamentos P2P, transferências internacionais de remessas, microtransações, contratos inteligentes, tokenização de ativos, entre outros. Contudo, a adoção generalizada é prejudicada por diversos desafios. Em suma, as criptomoedas representam uma inovação significativa com o potencial de revolucionar a economia global. No entanto, para que esse potencial seja plenamente realizado, é fundamental abordar os desafios existentes de forma integrada e colaborativa. A implementação de políticas regulatórias claras, o desenvolvimento contínuo de tecnologias avançadas, a melhoria da segurança digital, a construção de infraestruturas acessíveis e a promoção de educação são passos cruciais para facilitar uma adoção mais ampla e sustentável das criptomoedas. A pesquisa identificou áreas para estudos futuros, incluindo a evolução das regulamentações globais, o desenvolvimento de tecnologias escaláveis e a promoção da interoperabilidade entre plataformas. Esses esforços são essenciais para realizar o potencial das criptomoedas como um instrumento transformador nas finanças globais e no cotidiano das pessoas.

Palavras-chave: criptomoedas; blockchain; sistemas monetários; mercado financeiro; evolução financeira.

ABSTRACT

The objective of this research is to investigate the challenges and prospects for the adoption of cryptocurrencies in everyday life. The analysis focuses on identifying the potential benefits, practical uses, and technical, regulatory, security, educational, and infrastructure obstacles that influence the widespread acceptance and integration of cryptocurrencies. A narrative literature review methodology was used, covering a wide range of literature on cryptocurrencies, blockchain, financial technology, digital security, regulation and financial education. The research was based on platforms such as BDTD, SCiELO, Periódicos, IEEE, ACM, as well as data from online sources such as Statista and the World Bank.The results indicate that cryptocurrencies have significant potential to transform the global economy and people's daily lives. They have been used in a variety of practical applications, including P2P payments, international remittance transfers, microtransactions, smart contracts, asset tokenization, among others. However, widespread adoption is hampered by several challenges. In short, cryptocurrencies represent a significant innovation with the potential to revolutionize the global economy. However, for this potential to be fully realized, it is essential to address existing challenges in an integrated and collaborative way. Implementing clear regulatory policies, continually developing advanced technologies, improving digital security, building accessible infrastructure, and promoting education are crucial steps to facilitating broader and more sustainable adoption of cryptocurrencies. The research identified areas for future study, including evolving global regulations, developing scalable technologies, and promoting cross-platform interoperability. These efforts are essential to realizing the potential of cryptocurrencies as a transformative instrument in global finance and people's everyday lives.

Keywords: cryptocurrencies; blockchain; monetary systems; financial market; financial evolution.

SUMÁRIO

1 INTRODUÇÃO

Em retrospectiva histórica, os mercados em geral e mercados financeiros em particular experimentaram um grande desenvolvimento. Nesse sentido, os instrumentos utilizados como procedimentos tributários também sofreram alterações e evoluíram de acordo com necessidades do mercado, visando tornar, assim, transações comerciais e os direitos do Estado o mais simples possível, à luz do direito brasileiro (Raj, 2019).

Esses instrumentos usados para intermediar a troca de mercadorias são conhecidos como dinheiro. A maioria dos economistas define este como algo de meio de troca, uma unidade de contabilidade e uma reserva de valor. O dinheiro é um meio de troca no sentido de que todos concordamos em aceitá-lo ao fazer transações. Os comerciantes e Estado concordam em aceitar dinheiro em troca de suas mercadorias; os funcionários concordam em aceitar dinheiro em troca de seu trabalho. Como unidade de contabilidade, o dinheiro fornece dispositivo simples para identificar e para comunicar um valor bem como se trata de uma reserva de valor, pois permite armazenar as recompensas de trabalho ou negócio em ferramenta conveniente (Lewis, 2018; 2019; Campbell-Verduyn, 2018; Lantz & Cawrey, 2020). Em outras palavras, o dinheiro nos permite armazenar o valor de uma longa e árdua semana de trabalho em uma pequena pilha de dinheiro (Lewis, 2018).

Da era da troca ao dinheiro *commodity*, metal e moedas, ao ouro e prata, continuando pelos sistemas monetários modernos e terminando ainda com mais recentes desenvolvimentos monetários globais, como a introdução de dinheiro digital a partir de aplicativos e sistemas web e similares, passaram séculos. Cada tipo de dinheiro desempenhou um papel indispensável nas atividades de transação no respectivo período de tempo **(**Campbell-Verduyn, 2018). No entanto, como a sociedade humana em geral e mercados em particular evoluíram, houve a necessidade de instrumentos de troca de mercadorias mais sofisticados: aqui, a introdução de criptomoedas revolucionou o sistema de pagamento internacional em uma escala que poucos anos atrás era inimaginável (Lantz & Cawrey, 2020).

Atualmente, o planeta está marcado pelo desenvolvimento/uso intensivo da tecnologia blockchain, que maximiza potencial de tecnologias existentes para melhorar todos os negócios globais. Este é o próximo nível de globalização, que envolve e descentraliza o poder e reduz ainda mais o impacto do tempo e do espaço nas transações globais, sendo seu carro-chefe dessas novas tendências são as chamadas Criptomoedas (Lantz & Cawrey, 2020; Lewis, 2018). Mas, mesmo com essa frequente popularização, pouco se conhece ainda sobre as aplicações gerais do cotidiano e, não por menos, dos desafios subjacentes da criptomoeda.

Dessa forma, a presente pesquisa tem como pergunta principal: “quais são os desafios e as perspectivas para a adoção das criptomoedas no cotidiano?”. Este questionamento surge da necessidade de compreender como as criptomoedas, apesar de sua crescente popularidade e potencial revolucionário, ainda enfrentam barreiras significativas que impedem sua aceitação ampla e sua integração total no dia a dia das pessoas. De fato, as criptomoedas têm o potencial de transformar a economia global, oferecendo hoje uma alternativa descentralizada ao sistema financeiro tradicional, mas para isso é necessário superar uma série de desafios complexos e interconectados, fundamentalmente.

O objetivo desta pesquisa é investigar os desafios e as perspectivas para a adoção das criptomoedas no cotidiano, com foco em identificar benefícios, usos cotidianos reais bem como os obstáculos técnicos, regulatórios, de segurança, educacionais e de infraestrutura que afetam sua aceitação e uso generalizado. Além, buscou-se explorar as possíveis soluções e iniciativas que podem facilitar essa adoção. Apresentaram-se diversos cenários de aplicação hoje no Brasil, em consonância com estudos e dados, partindo-se para a investigação das lacunas e, não por menos, dos desafios. Assim, no âmbito técnico, a pesquisa pretendeu analisar questões diretas como a escalabilidade das redes blockchain, a interoperabilidade entre diferentes criptomoedas e a usabilidade das plataformas de transação.

No aspecto regulatório, o estudo investigou falta de clareza/consistência nas legislações, que muitas vezes varam entre países e até mesmo dentro de regiões do mesmo país, criando um ambiente incerto para investidores e usuários. Não por menos, para o que tange à segurança, a pesquisa se concentrou em problemas como a vulnerabilidade a ataques cibernéticos, fraudes e o roubo de criptomoedas, que continuam sendo uma preocupação central para os usuários. Em termos de infraestrutura, investigou-se a necessidade de uma rede robusta e ainda acessível para suportar o uso generalizado de criptomoedas, especialmente em regiões com menos acesso à tecnologia avançada. Além disso, o estudo explorou o papel da educação e da conscientização na adoção das criptomoedas.

A pesquisa adotou uma metodologia de revisão bibliográfica narrativa. Foi realizada revisão extensa da literatura existente sobre criptomoedas, blockchain, tecnologia financeira, segurança digital, regulamentação e educação financeira, considerando plataformas gerais de periódicos como BDTD, SCiELO, Periódicos, IEEE e ACM. Foram estas plataformas, também se investigaram dados recentes de blockchain e criptomoedas, a partir de plataformas online, como a Statista e Banco Mundial. O tipo de análise foi de conteúdo, a partir da perspectiva de Bardin (2011). Assim sendo, a pesquisa se dividiu em mais três seções, onde a primeira traz a vertente teórico-conceitual, depois as aplicações e, por fim, conclusão.

2 CONCEITOS E FUNDAMENTAMENTOS TEÓRICO-CONCEITUAIS DE BLOCKCHAIN E CRIPTMOEDAS À LUZ DA TI E DA TEORIA ECONÔMICA

Criptomoeda é uma moeda puramente virtual ou eletrônica, fundamentalmente sem uma garantia de *commodities* físicas e/ou obrigações soberanas. Em vez disso, esta depende de uma combinação de proteção criptográfica e protocolo ponto a ponto a testemunhar assentamentos. Consequentemente, possui propriedade não intuitiva de que, embora a propriedade do dinheiro seja implicitamente anônima, seu fluxo é globalmente visível (Lantz & Cawrey, 2020). Mas, para entender o que é uma criptomoeda em propriedade, é necessário entender, previamente, o que é a tecnologia *blockchain*, investigada nessa seção, seguida da caracterização objetiva da Criptomoeda e da sua posição como moeda na perspectiva econômica.

2.1 A TECNOLOGIA BLOCKCHAIN

2.1.1 A Descentralização da Confiança

Desde os tempos antigos, comerciantes têm usado livros de registros, e/ou *ledgers* (em alemão: 'Register'), para acompanhar os bens que compraram, venderam e trocaram ao longo de suas rotas comerciais, a fim de reconciliar os bens vendidos com os pagamentos recebidos (Chowdhury, 2018). Ao fornecer um mecanismo simples e confiável para acompanhar ativos e pagamentos, os registros se tornaram um instrumento fundamental para organizar as sociedades modernas e suas atividades econômicas. Registros modernos documentam coisas tão diversas quanto saldos de contas, títulos de propriedade, direitos autorais ou votos. Eles estabelecem um registro confiável de identidades, direitos de propriedade, fluxos de ativos e fornecem suporte documental para acordos contratuais complexos.

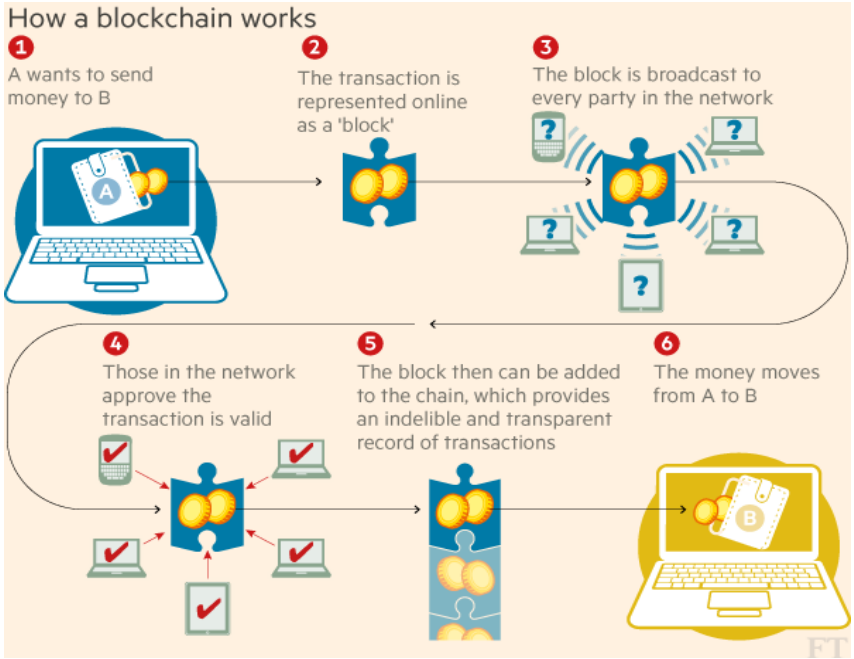
Até agora, a confiança entre atores realizando trocas econômicas nos mercados baseia-se em um sistema centralizado, ou seja, uma entidade que todos reconhecem como um terceiro de confiança (bancos, governos, empresas, notários, etc.). Essas entidades verificam identidade dos participantes em uma transação, supervisionam a compensação e liquidação e mantêm um registro das trocas". Tendo assim o monopólio da manutenção do registro, esses intermediários cobram taxas por seus serviços de verificação e autenticação. Consequentemente, eles têm um poder de mercado substancial devido a essa vantagem informacional (Chowdhury, 2018).

O problema é que essas instituições que cobram taxas e atuam como porteiros, ditando quem pode ou não se envolver em interações comerciais, adicionam custo e fricção às luzes das atividades econômicas de todos. Elas também têm o hábito de falhar com todos– pode-se pensar

na crise de 2008 como um caso de bancos quebrando seu dever de manter registros honestos – ou de explorar seu poder de coleta de pedágios para cobrar preços abusivos e exigir rendas exorbitantes. Em 2008, o mundo mergulhou em uma terrível crise financeira, testemunhando a instabilidade do sistema financeiro mundial estreitamente entrelaçado, mas também o perigo de confiar cegamente nos intermediários de confiança. Pouco depois, um misterioso livro branco foi publicado por uma entidade desconhecida usando o pseudônimo de Satoshi Nakamoto. Sua pesquisa, Bitcoin: A *Peer-to-Peer Electronic Cash System*, descrevia um sistema de pagamento mundial funcionando sem uma autoridade central, um instrumento de pagamento eletrônico que permite armazenar e trocar moeda digital (eletrônica) na forma de *token*. Tecnologia subjacente ao Bitcoin, a tecnologia blockchain, também chamada de tecnologia do livro-razão distribuído (DLT), oferecia registro digital infalsificável, permitindo registrar todas as transações realizadas em bitcoin (Chowdhury, 2018).

Enquanto uma entidade central atualiza o histórico de transações em moeda fiduciária, as transações em bitcoin são verificadas unanimemente por uma rede de usuários conectados. Ao contrário das redes centralizadas nas quais servidor central armazena e distribui informações para outros computadores na rede (chamados de 'nós'), a blockchain opera em rede distribuída peer-to-peer (P2P). Cada usuário da rede constitui um nó, estando conectado a vários pares, formando assim uma rede distribuída P2P. Uma transação pode, portanto, ser realizada entre dois pares, sem precisar ser autenticada por uma agência central, conforme se aponta através da Figura 1, apresentada a seguir.

Figura 1: Esquema de Blockchain



Fonte: Retirado de *World Economic Forum* (2024)

Pode-se definir a blockchain do Bitcoin como uma base de dados (chamada de registro) “que registra em ordem as transações entre os usuários de uma mesma rede” P2P. Por padrão, seu registro é público, pois todos podem ter acesso. Seu registro também é distribuído, pois cada nó possui uma cópia da base de dados. Ela “baseia-se em uma descentralização completa do registro das transações”, ou seja, funciona sem um órgão central de controle. Devido à sua natureza descentralizada, ela também se caracteriza pela ausência de um ponto central de falha: “Se um nó falhar, todos os outros nós permanecem interconectados; os dados e as informações que circulam na rede são assim preservados”. Ela opera em uma rede distribuída P2P, pois todos os nós da rede comunicam diretamente de um computador para outro e também funcionam simultaneamente como cliente e servidor para outro (Chowdhury, 2018).

Blockchain é tecnologia de armazenamento/transmissão de informações descentralizada (funcionando sem um órgão central), que foi projetada para resolver os problemas de confiança e incerteza que sempre existiram nas trocas econômicas. Tradicionalmente, foram instituições formais que assumiram o papel de intermediários de confiança nas trocas econômicas. Agora, podemos reduzir incerteza utilizando tecnologia blockchain, pois ela permite descentralização da confiança graças à desintermediação da atualização do registro. A redução da incerteza baseia-se na infalsificabilidade do registro, pois qualquer elemento inserido nele é imutável. “Ao fornecer um registro descentralizado, confiável e imutável das transações, a plataforma permite que indivíduos e instituições colaborem, transacionem e compartilhem informações com níveis de confiança e transparência nunca antes vistos” (Bashir, 2020, p. 55).

2.1.2 Mecanismos da Blockchain

Blockchains são registros digitais que registram informações distribuídas entre uma rede de computadores, garantindo que cada computador tenha registros idênticos. As tecnologias de blockchain consistem em 2 componentes fundamentais: estruturas de dados criptograficamente vinculadas, redes peer-to-peer e protocolos de consenso. O protocolo subjacente ao Bitcoin – a blockchain – baseia-se em três mecanismos fundamentais. Primeiro, as transações realizadas entre os usuários da rede são carimbadas com data e hora, agrupadas em blocos e vinculadas de forma segura utilizando a criptografia (Rodrigues & Kurtz, 2019).

O resultado é uma cadeia de blocos de transações. Em seguida, a blockchain opera em uma rede distribuída P2P, na qual cada nó armazena uma cópia do registro, valida a integridade do registro e compartilha e sincroniza as atualizações. Finalmente, para alcançar um consenso sobre a validade das transações, os nós utilizam um protocolo de consenso – ou seja, “um

conjunto de regras que permite aos nós determinar quando adicionar novas informações à blockchain". O estado da base de dados reflete o consenso alcançado (Pérez-Solà et al., 2019), fundamentalmente.

Quando um usuário deseja enviar fundos a outro usuário, ele se autentica com uma assinatura eletrônica, que se baseia na criptografia assimétrica. A criptografia assimétrica serve para proteger as trocas de informações, pois permite garantir a origem dos dados enquanto preserva sua confidencialidade. Primeiro, uma chave privada é gerada aleatoriamente, e essa chave é então usada para criar uma chave pública. Cada usuário possui esse par de chaves, sendo a privada conhecida apenas por seu proprietário, e a pública compartilhada com a rede. As chaves são funções matemáticas: a chave privada é usada para cifrar uma transação, enquanto a chave pública permite decifrar a transação (Furneaux, 2018).

Por exemplo, Paulo quer enviar 5 Bitcoin para Alice. Paulo usa sua chave privada para cifrar a mensagem "Paulo envia 5 BTC para Alice". A mensagem é cifrada, isto é, transformada em uma sequência de letras e números (por exemplo, AeF345Ksd54f34). A chave pública de Paulo permite decifrar a operação. Ao tempo, Paulo insere a mensagem cifrada no registro (AeF345Ksd54f34) e adiciona a sua chave pública, o que permite aos outros usuários da rede decifrar a mensagem usando a chave pública de Paulo. Paulo é, portanto, autenticado como o autor da transação. Como Paulo é o único a possuir sua chave privada, ele é o único que pode cifrar a transação que pode ser decifrada pela chave pública associada.

Assim, para realizar uma transação, o emissor usa logo a chave pública do receptor para transferir fundos para ele – uma transação que será visível para todos os membros da rede. Esses últimos podem então verificar que o emissor era, de fato, o último possuidor direto dos fundos enviados. O receptor, por sua vez, assina a transação com sua chave privada para receber os fundos. Após ser 'assinada', cada transação é carimbada com data e hora, o que permite ter uma ordem cronológica das transações e evitar o problema da dupla despesa (o risco de um mesmo montante ser gasto duas vezes). "As transações são registradas em blocos, sendo cada bloco vinculado cronológica e criptograficamente aos anteriores, criando assim uma longa cadeia de registros imutáveis (Edmunds, 2020, p. 314). Explora-se mais de perto como, de fato, funciona o processo de validação de blocos.

2.1.3 Blockchain como Organização Socioestrutural em Blocos

Dentro da blockchain, alcançar consenso entre partes não confiáveis é transformação do problema dos generais bizantinos. Este último refere-se à situação em que as partes envolvidas

devem concordar com uma estratégia única para evitar um fracasso total, mas onde algumas partes não são confiáveis. Alcançar um consenso em uma rede distribuída, particularmente em um ambiente sem confiança, é um desafio particular. Portanto, protocolos de consenso devem ser implementados para garantir a integridade do registro, sem passar pela intermediação de uma autoridade central (Shrivastava et al., 2020).

Segundo Nakamoto, um consenso poderia ser gerado incentivando os participantes da rede a resolver um quebra-cabeça criptográfico que exige cálculos intensivos e grande potência energética, tornando-o caro em recursos como energia, componentes de hardware e tempo – e, portanto, desencorajando os atores a se comportarem de uma maneira desonesta. A competição mantém assim a integridade do registro, criando confiança entre os participantes. Existem vários protocolos de consenso, mas o primeiro a surgir foi o usado pelo Bitcoin, a prova de trabalho: "Produzir prova de trabalho pode ser um processo aleatório com baixa probabilidade, de modo que muitas tentativas e erros são necessários, em média, antes que uma prova de trabalho válida seja gerada" (Daskalakis & Georgitseas, 2020 p. 55).

Concretamente, são indivíduos chamados 'mineradores' que validam as transações em processo denominado 'mineração' com computadores especializados. É necessário distinguir os nós – usuários que armazenam o registro e podem consultar as transações registradas nele – daqueles que validam blocos de transações e têm poder de escrever no registro (mineradores). Ambos podem ser pessoas físicas ou jurídicas. Uma vez que um bloco é ainda validado por um minerador, a transação torna-se visível para todos os nós, que a adicionam ao seu registro – este bloco será então permanente e imutável (Bashir, 2020).

Este processo distribuído substitui o intermediário de confiança do modelo centralizado, pois mineradores competem usando, assim, seu poder de computação para validar, por consenso majoritário, os blocos de transações aproximadamente a cada 10 minutos. O primeiro minerador a validar um bloco de transações é recompensado em Bitcoin. Os mineradores restantes devem então concordar com esse mesmo bloco de transações. Essa prova de trabalho é difícil de produzir, mas fácil de verificar para os nós. Além dessa remuneração, os mineradores também cobram taxas de transação (Vaneetvelde, 2018).

2.1.4 Sucesso no Quebra-Cabeça Criptográfico

O sucesso no quebra-cabeça criptográfico “consiste em obter um ‘hash’ do bloco que o minerador deseja integrar” ao registro – ou seja, converter, com função de hash, “um conjunto de dados numéricos em sequência binária curta que lhe é própria” (por exemplo, S4hk23L5ef).

O hash de blockchain é feito a partir do conteúdo do bloco, ou seja, “o hash do bloco anterior, um certo número de transações e um carimbo de data/hora”. “A função de hash SHA-256 é estruturada de forma que existem 2^256 combinações possíveis”. Logo, é impossível “produzir o mesmo hash duas vezes para dois conjuntos de dados diferentes”. Também é impossível modificar o conteúdo de um bloco, pois ele está sempre ligado aos blocos anteriores (qualquer modificação de um bloco é, portanto, refletida nos seguintes). “Consequentemente, modificar o conteúdo de um bloco requer recalcular os *hashes* de todos os blocos subsequentes”, o que é impossível, pois requer uma potência de cálculo inimaginável (Antonopoulos, 2015; Jordan, 2020; Bashir, 2020).

Quando um consenso é alcançado sobre o valor algorítmico do hash, o bloco validado é então transmitido de par a par para cada nó da rede, que o adiciona ao seu registro. As transações no novo bloco serão, a partir de então, imutáveis. Se um minerador tentar introduzir um bloco inválido, este não será validado pela maioria dos mineradores (mesmo que alguns possam ser mal-intencionados) e, portanto, não é adicionado ao registro nem transmitido aos pares. Isso permite proteger contra o risco de um ataque mal-intencionado em um sistema descentralizado. Essa segurança é um dos aspectos essenciais da blockchain. Além disso, devido ao design da tecnologia, dificuldade de encontrar novo hash aumenta ao longo do tempo, proporcionalmente ao número de entradas na blockchain. Da mesma forma, a recompensa em Bitcoin que os mineradores recebem tende a diminuir com o tempo (Antonopoulos, 2015).

Em resumo, a força da tecnologia blockchain decorre diretamente desses três fatores e da maneira como interagem: natureza distribuída do registro fornece transparência e também a sincronização; o protocolo de consenso elimina a necessidade de confiança; e a maneira como os dados são registrados, armazenados e conectados fornece imutabilidade e rastreabilidade, em fundamento (Jordan, 2020; Bashir, 2020).

2.1.5 Blockchains Públicas e Privadas

A blockchain pública é totalmente descentralizada. Por padrão, ela é de acesso aberto, ou seja, todos “os nós da rede têm acesso completo em tempo real aos dados” do registro, e qualquer minerador pode participar do processo de validação, sem obter autorização prévia de um terceiro. A confidencialidade é assegurada, pois a identidade dos nós e dos mineradores é protegida. A transparência é garantida, pois as transações são totalmente visíveis para todos os nós. A resiliência do registro é garantida, pois cada nó possui uma cópia do registro e não há ponto central de falha (Jordan, 2020; Bashir, 2020).

Como os mineradores são incentivados a se comportar de maneira honesta através de mecanismos econômicos de consenso, essas blockchains são resistentes à falsificação, o que garante a integridade dos dados. No entanto, essas blockchains são menos eficientes e rápidas, pois o número de validadores do registro é maior (Bashir, 2020).

A blockchain privada é totalmente centralizada. Ela é de acesso fechado, já que apenas um número definido de nós tem acesso ao registro e somente um conjunto amplo selecionado de mineradores é responsável pela validação dos blocos. Cada nó e minerador são autenticados e suas identidades são conhecidas pelos outros (Bashir, 2020).

As blockchains privadas podem também ser divididas em duas subcategorias: aquelas que são totalmente privadas, com uma organização que determina quem pode acessar o registro ou participar do processo de validação; ou aquelas que são formadas por um consórcio, ou seja, geridas por um número pré-selecionado de nós que correspondem a entidades privadas, como bancos. A blockchain do consórcio é parcialmente centralizada. Como o número de validadores do registro é menor, as blockchains de acesso restrito são mais eficientes e rápidas, mas isso ocorre em detrimento da transparência, segurança e imutabilidade dos dados (Jordan, 2020) – fundamentalmente.

2.1.6 Tipologias de Uso da Blockchain

Até agora, explicou-se principalmente todo o funcionamento da primeira aplicação da tecnologia blockchain – o Bitcoin. No entanto, qualquer domínio que tradicionalmente envolve a chamada de um terceiro de confiança pode ser transformado pela blockchain. Os domínios de aplicação da blockchain hoje são extremamente variados. Além do setor financeiro, existem serviços nos setores de energia, comércio, de transporte e logística, gestão de direitos digitais, saúde, administração e governo (Van Flymen, 2020).

Pode-se distinguir, de fato, três tipologias para os usos da blockchain: criptomoedas e carteiras digitais permitem contornar o sistema bancário tradicional nas transferências de ativos financeiros; a tecnologia do registro distribuído permite registrar qualquer tipo de informação de forma imutável e assim garantir a rastreabilidade e ainda a transparência da informação; e os contratos inteligentes oferecem a possibilidade de automatizar comunicações e transações entre as partes, executando ações previamente validadas pelas partes interessadas. Um contrato inteligente não é necessariamente um contrato no sentido jurídico do termo. Ele é mais uma modalidade técnica de execução de um contrato (Van Flymen, 2020; Garewal, 2020), que hoje – cada vez mais – vem surgindo em aplicação.

Como os contratos inteligentes práticos são uma tecnologia relativamente nova, ainda não está claro até que ponto são juridicamente vinculantes ou como devem ser interpretados. Em muitos casos, a jurisdição nem sequer será clara e, até onde se sabe, ainda não houve um caso em que um juiz tenha decidido sobre a interpretação de um contrato inteligente (Bashir, 2020; Van Flymen, 2020; Garewal, 2020).

O Ethereum foi a primeira blockchain a suportar a execução de contratos inteligentes. Estes são protocolos informáticos que permitem executar os termos de contrato, contornando assim os intermediários envolvidos na transferência de ativos, como advogados e bancos. Por isso, eles têm o potencial de perturbar o processo de transação, executando automaticamente os contratos de forma econômica, transparente e segura. Hoje, eles também podem ser usados para controlar títulos de propriedade privada material ou imaterial. Eles se beneficiam das mesmas características da blockchain: "sua execução é irrevogável e seu código é verificável livremente pelos nós da rede" (Van der Auwera et al., 2020).

2.2 CRIPTOMOEDA AO OLHAR DA PERSPECTIVA ECONÔMICA

2.2.1 Fundamentação Histórico-Construtiva

Foi inicialmente introduzida na sociedade, em grande impacto, em 2008. E desde então, experimentou um grande boom e gerou milhões de lucros para aqueles que estão envolvidos neste negócio. Chowdhury (2018) explica seu funcionamento da seguinte forma: criptomoeda pode ser pensada como uma cadeia de transações de um proprietário para o próximo, onde os proprietários são identificados por chave pública daqui em diante, um endereço que funciona como pseudônimo; ou seja, os usuários podem usar qualquer número de endereços e também sua atividade usando um conjunto de endereços não está inerentemente ligada à sua atividade usando outro conjunto ou à sua identidade no mundo real.

Em cada transação, o proprietário anterior assina com a chave de assinatura secreta correspondente ao seu endereço um *hash* da transação em que recebeu os bitcoins e o endereço do próximo proprietário ao passo que, ainda, segundo Rodrigues & Kurtz (2019), as transações podem ter muitos endereços de entrada e saída, ampliando a cadeia de provisão de saldos e, inclusive, dificultando reconhecer quais os verdadeiros donos de um patrimônio. Esta assinatura (ou seja, transação) pode então ser adicionado ao conjunto de transações que constitui a moeda; como cada uma dessas transações faz referência à transação anterior (ou seja, ao enviar bitcoins, o proprietário atual deve especificar de onde eles vieram), as transações formam uma cadeia. E neste ditame, a fim de verificar sua validade, um usuário pode verificar a validade de cada uma

das assinaturas nesta cadeia (Rodrigues & Kurtz, 2019). Buscando determinar qual transação veio primeiro, as transações são agrupadas em blocos, que servem para registrar a data e hora das transações que contêm e garantir sua validade. Os próprios blocos são formados em cadeia, com cada bloco fazendo referência ao anterior (e assim reforçando ainda mais a validade de todas as transações anteriores). Esse processo produz uma cadeia de blocos, que fica disponível publicamente para todos os usuários do sistema e garantem *celeridade* as criptomoedas (Pérez-Solà et al., 2019), fundamentalmente.

Historicamente, a criptografia foi usada principalmente por militares, serviços secretos e agências de inteligência como proteção contra o vazamento de informações classificadas., e a maioria dos acadêmicos da área tecnológica acredita que uma moeda digital autônoma que não esteja conectada a nenhum governo ou outro intermediário, como um banco, é atraente devido ao anonimato e à liberdade que oferece (Furneaux, 2018; Edmunds, 2020; Shrivastava et al., 2020; Daskalakis & Georgitseas, 2020). Afinal, a transferência de dinheiro entre regiões geográficas tanto domésticas quanto internacionais pode ser realizada de forma fácil e rápida, sem se preocupar com as regulamentações governamentais.

Existem opiniões diferentes e conflitantes sobre as criptomoedas em geral e de bitcoins em particular. Enquanto aqueles com visões libertárias da vida são otimistas e também abraçam o sistema de criptomoeda, outros autores, economistas e/ou estudiosos desse campo não estão entusiasmados com o uso da criptocurência no sistema de pagamentos e transações financeiras (Furneaux, 2018), pelo perigo que, em tempo, pode oferecer dentro dos sistemas financeiros e, subitamente, pela dificuldade em estabelecer sistemas tributários. Existe bastante divergência nas doutrinas econômicas, portanto.

A visão otimista do uso de criptomoedas é apoiada por estas facilitarem as transferências de fundos entre duas partes em uma única transação; essas transações são facilitadas pelo uso de chaves públicas e privadas para fins de segurança bem como são feitas com, a fato, taxas de processamento mínimas, permitindo aos usuários evitar as altas taxas cobradas pela maioria dos bancos (Antonopoulos, 2016). Além disso, diversos países começaram a aceitar criptomoedas como moeda válida. Um argumento que os promotores usam é a capitalização de mercado das criptomoedas, alegando que se tornou muito grande e poderoso, portanto, bani-los seria muito caro para qualquer país, incorrendo em amplificados prejuízos; logo, devem tanto direito quanto política e sociedade estudar maneiras de incorporá-los aos direitos fundamentais, coletivos e seus aspectos ético morais (Antonopoulos, 2016).

Por outro lado, os oponentes das criptomoedas afirmam que as criptomoedas são muito voláteis, podem ser usadas para lavagem de dinheiro e/ou financiamento de atividades ilegais.

Nesse sentido, Edmunds (2020), por exemplo, não se entusiasma com o uso de criptomoedas, apresentando razões pelas quais acredita que bitcoins não são uma moeda eletrônica viável. Ele observa que bitcoins são ilíquidos e mostraram alta volatilidade, e que o valor em dinheiro descontado de uma bitcoin é zero. E ainda afirma que a moeda carece de um emissor central e que não há base financeira ou econômica a sua criação. Shrivastava et al. (2020), neste campo de diferenças e caracterizações, fornece as vantagens e desvantagens das criptomoedas frente ao mercado comum do dinheiro (moeda tácita, que apresenta lastro), a partir de seus respectivos resultados operacionais, jurídicos e estruturais. Veja-se, pois, que a dualidade é uma realidade na discussão da criptomoeda.

2.2.2 De Um Projeto Político a Um Projeto Técnico

Para entender todos os fundamentos técnicos das criptomoedas, é necessário primeiro compreender suas raízes políticas e sociais. Originalmente, as criptomoedas buscam inspiração nos pensamentos dos libertários e dos *cypherpunks*. Os primeiros procuram estabelecer − ou melhor, restabelecer − a separação entre o Estado e a moeda, enquanto os segundos defendem a privacidade através da criptografia (Antonopoulos, 2014).

Essas comunidades de pensamento se interessam pela moeda, pois ela está no centro de toda atividade econômica e, portanto, de parte importante da atividade humana. Ela intervém nas trocas comerciais, nos contratos, nos investimentos e na relação entre os cidadãos e Estado. Até mesmo estruturas familiares ou religiosas, por natureza não comerciais, não podem escapar completamente disso (Judmayer et al., 2017).

O controle da moeda é, intrinsecamente, um controle da sociedade. É um controle da economia, primeiramente, através da política monetária, e isso mesmo que a criação de bancos centrais independentes tenha feito muito para restringir, assim, todos os abusos históricos do *seigniorage*. É também, mais recentemente, um controle dos indivíduos através da digitalização dos pagamentos e da transformação do sistema bancário em um panóptico eletrônico (Judmayer et al., 2017). Esse poder de controle representa uma vantagem e uma segurança para os poderes públicos, especialmente em termos de combate ao crime ou coleta de impostos, mas também pode representar um risco considerável para as liberdades públicas (Antonopoulos, 2014).

Por um lado, a segurança dos dados em larga escala é dificuldade por vezes subestimada. Sistemas eletrônicos são regularmente violados por grupos criminosos ou governos estrangeiros para fins de espionagem econômica. Uma empresa francesa não pode mais contar hoje com a confidencialidade de suas transações e, portanto, a fortiori, com a de seus fornecedores, clientes,

deslocamentos de seus executivos, etc (Furneaux, 2018). Esse argumento remete às *crypto wars* dos anos 1990, que resultaram na liberalização das tecnologias (TI) de criptografia nos Estados Unidos (Furneaux, 2018).

Em 1993, diante do crescente interesse da indústria pela criptografia, a NSA propôs o chip *Clipper*. Esse chip permitia que os civis tivessem acesso a tecnologias de criptografia até então reservadas ao exército. Como o compromisso, o chip incluía abertamente uma porta dos fundos, permitindo que os serviços de inteligência e as forças de ordem decifrassem qualquer comunicação. Em menos de um ano, o algoritmo foi quebrado pelo criptógrafo *Matt Blaze*, que demonstrou que a porta estava assim na verdade escancarada. Os poderes públicos americanos acabaram por aceitar a evidência: as matemáticas são neutras, não distinguem as intenções de seus usuários. Restringir as tecnologias de criptografia é em vão, ou em detrimento da segurança de todos. A confidencialidade é absoluta ou não é (Furneaux, 2018).

Por outro lado, diante de questões tão importantes, não parece prudente nem razoável supor a priori a benevolência de todos os poderes públicos. Isso não se trata de uma paranoia e teoria da conspiração, mas simplesmente, de fato, da aplicação do princípio da precaução. Essa abordagem cautelosa tem antecedentes históricos bastante respeitáveis, como a ratificação da Constituição americana ou a Declaração dos Direitos do Homem e também do Cidadão de 1789 (Furneaux, 2018). Para tomar um exemplo menos imponente, a independência legal dos bancos centrais, mencionada acima, tira claramente lições da história ao retirar dos governos seu poder discricionário sobre a emissão de moeda. Mas, muito além da política monetária, também é necessário se proteger contra o risco totalitário (Antonopoulos, 2014).

Em 2017, mais da metade da população mundial vivia sob o jugo de regime autoritário; 44% estavam sob a autoridade de um *x* ditador. Esses regimes modernos dispõem de recursos tecnológicos consideráveis. Com o controle completo dos pagamentos eletrônicos, o governo chinês desenvolve hoje sistemas de vigilância orwellianos que avaliam os cidadãos com base em seus hábitos de consumo, suas associações, e/ou suas posições políticas. A Venezuela hoje utiliza a mesma tecnologia. Qual será o impacto do controle absoluto dos intercâmbios durante uma limpeza étnica? Esses riscos são reais e não podem ser ignorados, inclusive, hoje, na esfera ocidental (Roos, 2022).

O risco político e risco econômico associado ao sistema monetário não é, parafraseando *Soljenítsin*, o sinistro desígnio de homens de alma negra. Ele reflete a limitação tecnológica fundamental. Historicamente, e até muito recentemente, a transmissão de moeda à distância era feita ou pelo transporte de dinheiro físico ou também pelo crédito interbancário (Roos, 2022; Antonopoulos, 2014).

Para proteger as liberdades individuais, as criptomoedas propõem uma alternativa a esse sistema, onde o dinheiro se torna eletrônico. Elas tornam o pagamento à distância possível sem recorrer ao crédito e, portanto, sem recorrer ao sistema bancário e ao aparato governamental necessário para fazer cumprir todo o pagamento das dívidas. A construção dessas criptomoedas repousa sobre décadas de pesquisa em criptografia e computação distribuída (Garcia-Alfaro et al., 2017), fundamentalmente.

2.2.3 A Assinatura Digital: A Pedra Angular Do Edifício

Em 1976, Whitfield Diffie e Martin Hellman descrevem a noção de assinatura digital e ampliam campo de aplicação da criptografia além da criptografia/descriptografia. A criptografia geralmente tem como seu objetivo preservar a confidencialidade das mensagens; as assinaturas digitais atestam sua autenticidade. Essas assinaturas são infalsificáveis, inalteráveis e também irrevogáveis. Elas comprovam, de fato, a posse de chave privada, um dado digital conhecido apenas pelo signatário. Desde cartões inteligentes até sites da Internet, essas assinaturas digitais estão hoje onipresentes. Ao criar uma identificação matematicamente verificável para sistemas eletrônicos, essas assinaturas abrem a porta para uma moeda digital. No entanto, as tentativas de construir sistemas monetários descentralizados a partir de assinaturas digitais enfrentam o problema da dupla despesa. O restante deste artigo esboça alguns elementos-chave do design desses sistemas (Morgan, 2018).

2.2.4 Dupla Despesa: Uma Pedra De Tropeço

Para ilustrar esse ponto, tenta-se construção ingênua de sistema simplificado. Suponha-se que, inicialmente, por convenção, Alice seja a única detentora de moeda, dispondo de um crédito de 1.000$ (em moeda recorrente). Alice gasta essa quantia assinando digitalmente dois cheques, um que atribui 700$ a Oscar e outro que atribui 300$ para Bernardo. A validade da transação é assegurada pela autenticidade da assinatura de Alice e pelo fato de que 700 + 300 = 1.000. Suponha-se que, por sua vez, Oscar decida gastar os 700$ que recebeu de Alice. Oscar assina transação transferindo 700$ para Carol, mas também assina outra transação transferindo a mesma quantia para Bernardo. Essas duas transações são incompatíveis, mas, para perceber isso, Carol e Bernardo devem ter conhecimento das transações que um e que o outro receberam. Historicamente, sob o regime da moeda-ouro, esse tipo de problema não ocorre. São as leis da física que governam as contas: nada se perde, nada se cria (Gates, 2017; Isaacs, 2017; Girasa, 2018; Matharu, 2018).

Para as moedas fiduciárias, o mecanismo é tipicamente hierárquico, com uma autoridade central, banco central, que mantém um grande livro de contas para seus clientes, as instituições bancárias. No domínio de moedas descentralizadas, todavia, é o conhecimento comum de todas as transações por todos participantes que assegura toda a boa manutenção das contas. No plano técnico, todos os participantes devem concordar sobre a ordem das transações. De fato, vez que Carol aceitou a transação de Oscar, é necessário que o sistema possa ainda rejeitar a transação conflitante que Oscar poderia realizar em favor de Bernardo (Matharu, 2018). Isso supõe que todos os participantes reconheçam que uma das transações foi publicada antes da outra. A ordem escolhida não é, em si mesma, muito importante, mas é imperativo que seja incontestável – o que é necessário para a sociedade contemporânea (Morgan, 2018; Gates, 2017).

Na teoria do cálculo distribuído, tal problema é conhecido como problema do consenso. Ele modela um conjunto de processos que devem chegar a um acordo, em um tempo finito, sobre conteúdo de um registro representando histórico de transações. Variação particularmente difícil do problema trata da criação de protocolos de consenso na presença de participantes mal-intencionados, chamados bizantinos (Isaacs, 2017; Girasa, 2018).

Tais atores bizantinos agem à vontade, sem necessariamente seguir regras do protocolo; eles também podem corromper a rede retardando a circulação das mensagens. Nesse caso, os participantes honestos devem chegar a consenso apesar da presença desses atores desonestos. O problema é descrito pela primeira vez no artigo *The Byzantine Generals Problem*, que, ao considerar o caso mais geral, demonstra que o problema é solucionável se e somente se menos de 1/3 dos participantes forem bizantinos. Essa abordagem permite distribuir a responsabilidade pela manutenção das contas, mas depende da seleção de um conjunto fixo de participantes. Portanto, não é adequada para uma rede descentralizada em grande escala, que, por natureza, deve ser aberta a todos. A abertura da rede é particularmente problemática na presença de atores bizantinos. É fácil para um atacante, em uma rede aberta e anônima, se passar por várias partes diferentes e usar essa ilusão para fazer o consenso falhar, um ataque conhecido como ataque Sybil (Isaacs, 2017; Girasa, 2018).

2.2.5 Prova De Trabalho

Em 2008, Bitcoin propôs uma abordagem heterodoxa. A participação no consenso não se faz a partir de noção de identidade, mas provando o consumo de potência computacional. A técnica, conhecida como prova de trabalho, foi originalmente introduzida para limitar os spams

em e-mails pelo criptógrafo Adam Back e baseia-se no princípio da inversão parcial de uma função de hash criptográfica (Matharu, 2018).

A participação no processo de consenso do Bitcoin, portanto, não é assim sendo medida em "entidades" distintas, mas em potência computacional. Essa abordagem não só contorna os ataques Sybil, mas também se presta a mecanismo econômico que recompensa a participação honesta no protocolo e pune, assim, desvios bizantinos. A rede, portanto, tolera os participantes relativamente amorais que, buscando seu próprio interesse, contribuem para a segurança da rede ao "minar" os novos blocos criados pela prova de trabalho. Além das propriedades de segurança, essa prova de trabalho permite a distribuição inicial, anônima e imparcial de bitcoins para esses "mineiros" por cada bloco criado (Garcia-Alfaro et al., 2018; Tapscott & Tapscott, 2018; Lewis, 2023; Dupont, 2019; Grabowski, 2019).

É importante entender que os cálculos efetuados no âmbito da prova de trabalho não são intrinsecamente úteis. Eles não determinam a validade das transações, não atualizam uma base de dados. A prova de trabalho serve apenas para provar que os recursos reais, no caso energia, foram irrevogavelmente gastos. Apesar de suas vantagens evidentes, a prova de trabalho não está isenta de críticas (Garcia-Alfaro et al., 2018).

O criptógrafo Ben Laurie observou que, para garantir sua segurança, a prova de trabalho deve representar metade de toda a potência computacional mundial. O argumento assume uma posição extrema, mas é fato que, nos últimos anos, a potência dedicada ao bom funcionamento da rede tomou proporções consideráveis, na ordem de vários gigawatts. Para muito além disso, os argumentos a favor da prova de trabalho – especialmente seu aspecto descentralizado – são questionados tanto pela prática quanto por análises de teoria dos jogos (Tapscott & Tapscott, 2018; Lewis, 2018).

Um ataque, por exemplo, pode consistir em voltar atrás, ou seja, reescrever a história do blockchain. Se não é possível modificar o conteúdo dos blocos, é possível, no entanto, alegar que esses blocos nunca foram produzidos, ou que outros blocos foram produzidos. Tipicamente, um ataque assim só pode ter sucesso se mais de 51% dos mineradores participarem, pois essa cadeia "alternativa" deve superar em comprimento a cadeia original a ser considerada legítima (Dupont, 2019).

É custoso participar de um ataque destinado ao fracasso, mas um atacante estrategista pode subornar outros mineradores, oferecendo-lhes uma espécie de apólice de seguro em caso de revés, e uma pequena recompensa em caso de sucesso. Em um modelo onde os agentes são amorais e buscam cegamente o lucro, o seguro garante o sucesso do ataque e não custa nada ao atacante (Grabowski, 2019). Este exemplo não tem a intenção de insinuar que a rede não é

viável, mas sim de mostrar que a segurança da rede depende muito mais da honestidade dos participantes do que às vezes se faz parecer.

2.2.6 Prova De Participação

Uma outra abordagem do consenso – isso é, a prova de participação –, que é anterior ao Bitcoin, está ganhando destaque hoje em dia. A ideia é usar a própria moeda como mecanismo de resistência contra os ataques Sybil. A participação no consenso não é, assim, mais baseada na quantidade de poder computacional gasta, mas sim numa quantidade de moeda detida. Esta abordagem tem a falha de ser circular. A segurança do consenso é necessária para determinar os direitos de participação no consenso. Essa circularidade não pode ser completamente evitada e, portanto, prova de participação não pode replicar todas as propriedades de segurança exibidas pela prova de trabalho. Isso pode ser visto, de outro ângulo, através de um simples argumento de simulação (January, 2021).

Suponha-se, de maneira muito geral, que a criação de blocos não tenha custo. Esse é um dos objetivos da prova de participação. Nada impede, então, que os participantes maliciosos forjem em paralelo duas cadeias, uma pública e outra secreta. Esses atores podem, a qualquer momento, vender a moeda que possuem na cadeia pública e publicar, simultaneamente, sua cadeia secreta. Um novo participante que descobre o sistema verá então, de fato, duas cadeias: a autêntica e outra falsa. Nenhuma propriedade intrínseca da cadeia autêntica permite distingui-la da cadeia falsa. A duplicidade dos atores maliciosos pode ser detectada comparando as duas cadeias, e então poderia ser considerada uma punição. Sim, mas como, já que eles não têm mais nada em jogo, um problema conhecido como "*nothing-at-stake*" (Juraszek, 2020; Kapilendo, 2017), fundamentalmente.

O argumento está correto, mas, embora muitas vezes seja considerado logo o obstáculo insuperável para a prova de participação, não é necessariamente relevante. Para começar, assim, a maioria das abordagens de prova de participação automaticamente bloqueia os fundos dos participantes que produzem blocos. Se esses fundos, por exemplo, forem bloqueados por um mês, isso significa que durante esse período, deve-se garantir que uma cadeia "falsa" publicada na rede deve se divergir da cadeia autêntica (Juraszek, 2020; Kapilendo, 2017). Caso contrário, os atores maliciosos que criaram essa cadeia falsa podem ser punidos através da destruição de seus fundos (Juraszek, 2020; Kapilendo, 2017).

O critério de segurança se torna então o seguinte: os participantes do consenso devem se conectar à rede pelo menos uma vez por mês, e os novos participantes devem determinar um

estado recente da cadeia. Eles podem fazer isso consultando, de fato, comerciantes que aceitam a moeda em questão. Não se deve esquecer que a aceitação de uma moeda reflete sempre um consenso humano e social. Portanto, as *blockchains* não escapam dessa "subjetividade fraca", quer usem prova de trabalho ou prova de participação (Kapilendo, 2017). Por sua vez, a prova de participação apresenta propriedades únicas. Permite, em particular, uma assimetria para os participantes: a criação honesta de blocos é muito barata, enquanto as deviações do protocolo podem ser punidas severamente (Kapilendo, 2017).

Assim, reintroduz, de acordo com o clássico teórico Vitalik Buterin, uma assimetria característica da criptografia e do movimento *cypherpunk*, onde o ataque é muito mais custoso do que a defesa (Kapilendo, 2017). Devido às suas propriedades de segurança e baixo custo, a prova de participação representa uma opção diferente ao design de uma criptomoeda. Depois do sucesso do Bitcoin e da prova de trabalho, a prova de participação está hoje em dia ganhando um novo interesse. Suas propriedades "subjetivas" são assumidas, como no Tezos (um projeto no qual o autor está particularmente envolvido), que também busca superar as tensões de governança inerentes à prova de trabalho (Kapilendo, 2017).

Considerada ainda há alguns anos como uma impossibilidade, a prova de participação está no centro de uma nova geração de projetos como o Tendermint, que se baseia em algoritmos clássicos de acordo bizantino; o Polkadot, que leva, assim, ao limite possível o uso do cálculo distribuído conciliando agilidade e segurança; ou ainda o Algorand, uma blockchain projetada por Silvio Micali, um renomado criptógrafo detentor dos prêmios Gödel e Turing (Juraszek, 2020; Kapilendo, 2017).

3 CRIPTOMOEDAS NO BRASIL: DESAFIOS E PERSPECTIVAS

Relevantemente, para que se compreenda como se dá cenário de criptomoedas no Brasil, faz-se, de antemão, necessário entender cenário global. Dado que, hoje, o perfil demográfico do usuário de criptomoedas não é visível, estabelecer um quadro exato de onde as criptomoedas são utilizadas e em quais países o nível de atividade é mais alto constitui uma tarefa desafiadora, se não impossível. Para esta pesquisa, utilizam-se algumas plataformas centrais que hoje são as mais utilizadas pelos usuários

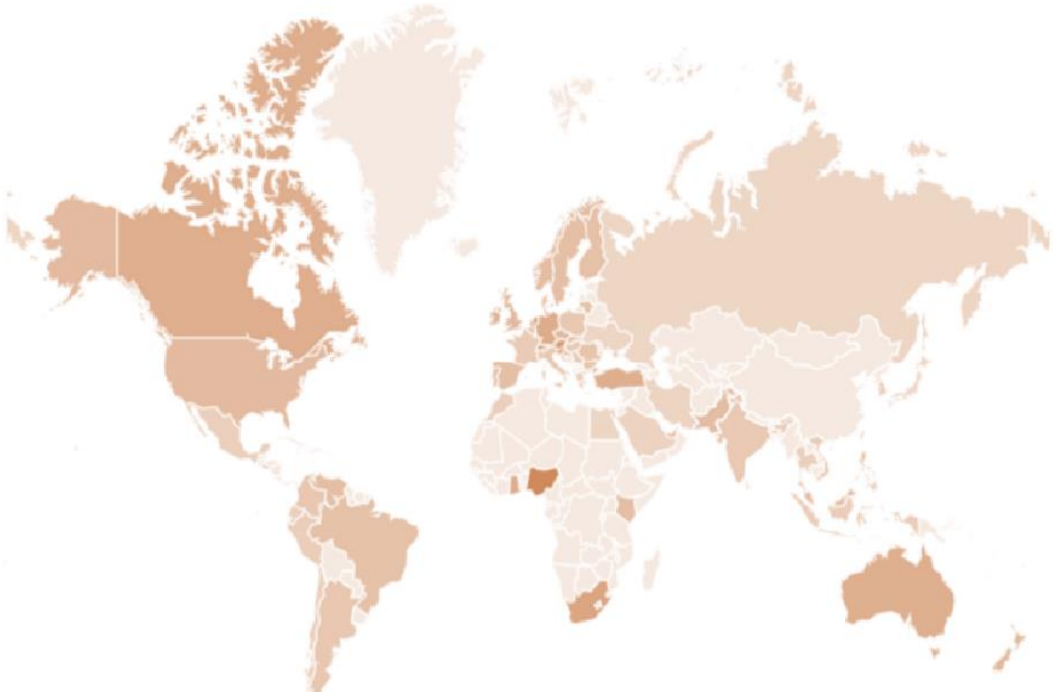
Nisso, fator fundamental a considerar é que o uso de criptomoedas é proibido em alguns países. Segundo *Coin.dance* (2024), o uso de criptomoeda é permitido em 132 países ao redor do mundo hoje. Atualmente, seu uso foi declarado ilegal por governos do Afeganistão, Argélia, Bangladesh, Bolívia, Paquistão, Macedônia do Norte e Vietnã, enquanto há restrições ao uso

nas Samoa Americanas, China, Egito, Marrocos, Nepal, Catar e também Zâmbia (*Coin.dance*, 2024). Já outros governos abraçaram plenamente as criptomoedas: em 2021, El Salvador foi o primeiro Estado a aprovar a “bitcoin” como moeda oficial, junto com o dólar americano. Alguns países compraram criptomoedas por conta própria (Bulgária, Ucrânia, El Salvador, Finlândia e Geórgia) (Vaneetvelde, 2018).

Existem, além disso, fontes de informações, embora parciais, que permitem identificar o uso efetivo das criptomoedas nos diferentes países. Como mencionado anteriormente, um indicador é o número de buscas sobre o tema no Google Trends. Nos últimos 5 anos, o maior número de buscas por "criptomoeda" foi registrado na Nigéria, seguido de El Salvador, Áustria, Países Baixos e Suíça. As tendências geográficas são ampliadas semelhantes para termos como "bitcoin" ou "moedas digitais", mas com volumes amplamente menores (Figura 2). Já uma outra métrica relevante é o número de nós por país que estão minerando bitcoin. Um nó é computador conectado a outros computadores que segue as regras e compartilha informações da blockchain de bitcoin ou criptomoeda (Vaneetvelde, 2018)

Localizar os nós é possível, já que a rede bitcoin é de código aberto. Atualmente, os Estados Unidos, Alemanha, França, Países Baixos e Canadá ocupam os primeiros cinco lugares em termos de número de "nós completos" de bitcoin (Figura 2). No entanto, deve-se notar que a origem de um nó completo pode ser obscurecida, e que a distribuição geográfica da mineração de bitcoin não está necessariamente ligada à distribuição geográfica das transações de bitcoin.

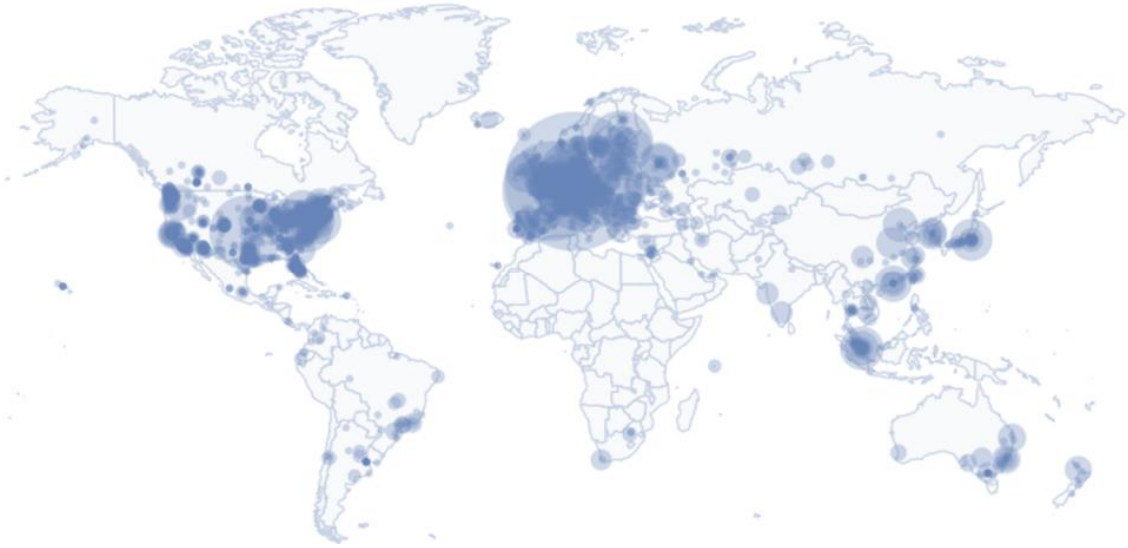
Figura 2: Distribuição do Bitcoin no Globo até o fim de 2022



Fonte: Retirado de Google Trends (2024)

Segundo o Coinmap (2024), uma plataforma que lista todas as localidades conhecidas que aceitam criptomoedas como forma de pagamento, observa-se concentração significativa de comerciantes na América do Norte e, em particular, na Europa (Figura 2). Algumas atividades também podem ser observadas na região Ásia-Pacífico (principalmente concentradas na Coreia do Sul, Japão e Austrália), América Latina (principalmente no Brasil e Argentina) e na África e Oriente Médio (particularmente no Quênia, África do Sul e Israel). No entanto, vale notar que apenas minoria de comerciantes que aceitam criptomoedas em todo mundo está representado no Coinmap, de fato. Com isto, tem-se a distribuição de nós, a seguir.

Figura 3: Distribuição geográfica de nós completos de Bitcoin



Fonte: Retirado de *Lewis* (2023)

Os dados sobre a localização dos downloads de software utilizados para o comércio de bitcoin mostram uma alta incidência, em percentual em relação à população, especialmente em países escandinavos (Estônia, Islândia, Suécia, Holanda e Dinamarca). Novamente, a utilidade desta métrica é limitada pelo fato de que nem todas as transações de bitcoin ocorrem por meio de software, e que nem todos os softwares são rastreados (Lewis, 2023)

LocalBitcoin é uma plataforma de troca de criptomoedas que conecta eletronicamente usuários em 249 países. Volumes de troca são limitados em comparação com outras plataformas maiores (como Binance ou Coinbase Exchange), mas o LocalBitcoin permite conhecer o país de origem e destino das trocas porque elas são realizadas em ATMs físicos distribuídos pelo mundo. 94% de todos ATMs conhecidos estão localizados nos Estados Unidos (59%), Europa (94-59-15) e Canadá (15%), mas nota-se um rápido incremento ao longo do tempo nos países emergentes da Ásia (China, Índia, Malásia, Tailândia), América Latina (como o Brasil, Chile,

Colômbia, México, Venezuela), África e Oriente Médio (Quênia, Nigéria, Arábia Saudita, Tanzânia, Turquia) e Europa Oriental (Rússia e Ucrânia) (Lewis, 2023). Por fim, um estudo (Bashir, 2020) que analisou as bases de dados proprietárias de alguns fornecedores de carteiras e plataformas de pagamento, que incluem informações sobre a localização dos clientes, revelou que quase 40% dos usuários de criptomoeda estão sediados na Ásia, seguida pela Europa com 27%, e que a América Latina tende a ter crescimento subsequente nos próximos anos. Assim, a participação relativa da América do Norte é surpreendentemente baixa e também não condiz com os números mencionados anteriormente (Bashir, 2020). No entanto, vale notar que esses números representam apenas os dados de um número limitado de fornecedores de carteiras e plataformas de pagamento e não levam em conta os usuários das trocas e também dos pools de mineração (Bashir, 2020).

Em conclusão, parece que a adoção de criptomoedas está mais avançada na América do Norte e na Europa, mas um número crescente de atividades (e usuários) pode ser observado também em outras regiões, com atividades crescendo relativamente rápido em alguns países emergentes da Ásia, América Latina, África e Oriente Médio. Ao mesmo tempo, nesses países é atualmente mais difícil rastrear o uso de criptomoedas, como no Brasil, que hoje é o principal mercado da América Latina, conforme visto a seguir.

3.1 MERCADO DE CRIPTOMOEDAS NO BRASIL

O mercado de criptomoedas está em constante evolução, e as projeções para os próximos anos indicam um crescimento significativo. De acordo com os dados da Statista para 2024, a receita no mercado de criptomoedas é projetada para alcançar US$ 1.094,0 milhões, com uma taxa de crescimento anual composta (CAGR) de 9,57% até 2028, atingindo um total projetado de US$ 1.577,0 milhões. Essa estimativa reflete não apenas a crescente aceitação e adoção das criptomoedas, mas também o potencial de expansão do mercado (Statista, 2024) – que vem de maior ocorrência após a normatização (Lei 14.478/22) (Statista, 2024).

A receita média por usuário no mercado de criptomoedas é estimada em US$ 23,6 em 2024. No entanto, os Estados Unidos se destacam como o país com a maior receita, prevista para atingir US$ 23.220,00 milhões no mesmo ano. Essa disparidade reflete a diferença na adoção e no uso de criptomoedas em diferentes regiões do mundo. Em termos de número de usuários, espera-se que o mercado de criptomoedas alcance 55,01 milhões de usuários até 2028, com uma penetração de usuários de 21,29% em 2024, aumentando para 24,77% até 2028. Esse

crescimento expressivo indica uma crescente aceitação e adoção das criptomoedas entre indivíduos e instituições em todo o mundo (Statista, 2024).

Entre os principais players do mercado de criptomoedas no Brasil, estão *Binance*, *ByBit*, *Coinbase*, *Crypto.com*, *Gate.io*, *Huobi*, *Kraken*, *Liquid* e *OKX*. Essas plataformas são as com o maior grupo de transações e de oferta de serviços relacionados às criptomoedas para os usuários em todo o mundo. Para muito além disto, a Statista (2024) aponta para o alto nível de *altcoins*, ou criptomoedas alternativas, que possuem características e casos de uso únicos. Essas altcoins representam uma oportunidade para os investidores diversificarem seus portfólios e explorarem novas oportunidades de investimento no mercado de criptomoedas, mas também estão, hoje – a se tornar um risco sistêmico pelas fraudes (Statista, 2024).

Conforme a plataforma Statista (2024), de fato, vários fatores estão impulsionando o crescimento do mercado de criptomoedas, incluindo a crescente aceitação e também a adoção de criptomoedas por indivíduos e instituições, o interesse crescente em plataformas de finanças descentralizadas (DeFi) e o potencial das criptomoedas como uma proteção contra a inflação e a instabilidade política. Além disso, os avanços na tecnologia blockchain e o aumento do uso de criptomoedas para transações transfronteiriças também estão contribuindo ao crescimento do mercado brasileiro (Statista, 2024).

3.2 PERSPECTIVAS, ADOÇÃO E BENEFÍCIOS DE USO AO COTIDIANO

3.2.1 Criptomoeda como Fator de Inclusão Financeira

A alteração da dinâmica microeconômica e financeira proporcionada por criptomoedas pode ser observada em várias funções que já são aplicáveis à realidade brasileira. Em primeiro lugar, as criptomoedas podem atuar como meio de pagamento, oferecendo alternativa eficiente e segura ao sistema bancário tradicional, especialmente às transações digitais e internacionais (Antonopoulos, 2015).

Isso é particularmente relevante no Brasil, onde a inclusão financeira ainda é um desafio significativo. Como apontam Timotio et al (2018, p. 17), “desigualdade é marcante no território brasileiro, já que o Sudeste e o Sul retornaram pontuações bem superiores à média nacional e, portanto, às demais regiões. Isso indica que ou maiores índices de crescimento econômico e bem-estar social contribuem para a elevação da inclusão financeira, ou a inclusão financeira contribui para o maior crescimento econômico e para a elevação do bem-estar social, ou seja, para o desenvolvimento socioeconômico.”

Novos sistemas de transação, caracterizados por uso de criptomoedas e carteiras digitais, possuem um atrativo particular para as populações desfavorecidas, pois são frequentemente menos dispendiosos que as transferências com o dinheiro móvel. Nos anos recentes, a indústria móvel tem investido e colaborado com *startups* para o desenvolvimento e implementação de projetos blockchain, em parceria com governos e atores do desenvolvimento. Quando usuários desejam comprar produtos ou serviços, eles utilizam uma carteira digital para enviar e receber criptomoeda ou trocá-la por moeda fiduciária. O uso de uma carteira digital em um telefone móvel equivale à abertura de uma conta bancária. Cada indivíduo torna-se, assim, seu próprio banco. Essas plataformas oferecem serviços semelhantes aos bancos, incluindo a compensação e liquidação de ativos financeiros, bem como produtos financeiros como seguros (Jordan, 2020; Bashir, 2020). No Brasil, isto está cada vez mais recorrente: como apresenta Menegatti et al. (2017), os consumidores brasileiros estão, cada vez mais, partindo para a utilização da carteira e dos meios digitais para realizar suas compras e aquisições, até mesmo mais básicas e, com o tempo, as criptomoedas estão se tornando um meio de financeira com lastro significativo para compor a seguridade operacional (Menegatti et al., 2017; Hosp, 2017).

Como o uso de criptomoedas ainda não é generalizado, a maioria das pessoas precisa realizar várias trocas de moeda a poder transacionar, o que introduz novos custos, especialmente nos países em desenvolvimento, onde há pouco ou nenhum mercado de troca de moeda local por criptomoeda. As transações se tornam caras ou, às vezes, impossíveis. Consequentemente, as plataformas de criptomoedas que estão oferecendo para os seus usuários a possibilidade de transacionar em qualquer moeda, real ou digital, estão garantindo a interoperabilidade entre diferentes operadores de dinheiro móvel, melhorando a inclusão digital no Brasil e ganhando, a cada dia, mais assinantes (Hosp, 2017).

Uma análise realizada em 2018 estudou o efeito das transações de Bitcoin sobre dois conceitos-chave que permitem às pessoas melhorar sua qualidade de vida: a inclusão financeira (medida por indicadores como a maneira como as pessoas poupam, tomam empréstimos, realizam pagamentos e gerenciam riscos) e o desenvolvimento humano (medido pelo Índice de Desenvolvimento Humano - IDH) – sendo a penetração da internet pré-requisito determinante (Lewis, 2018).

As transações de Bitcoin possibilitam o desenvolvimento econômico através da inclusão financeira do Brasil daqueles que, de outra forma, não teriam acesso aos sistemas de pagamento necessários para realizar transações financeiras. O uso de Bitcoin torna a inclusão financeira possível através dessa infraestrutura descentralizada porque opera em um sistema de registro

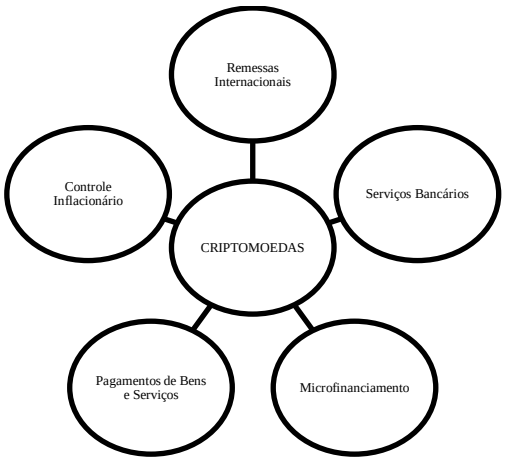
ponto a ponto, no qual as transações podem ser completadas sem um banco ou uma instituição financeira (Senna; Souza, 2023).

Hoje, a literatura (Campbell-Verduyn, 2018; Raj, 2019) está ciente de que o uso das criptomoedas não altera em nada as desigualdades estruturais inerentes às sociedades. Todavia, combinadas com as tecnologias móveis, as criptomoedas são instrumentos capazes de cobrir a população mal atendida, abrindo o acesso aos serviços financeiros com a ajuda de um simples telefone celular. Afirma Nordbo (2020, p. 541):

> Graças à automação e desintermediação do sistema de pagamento, à redução dos custos e à segurança das transferências, as comunidades periféricas e marginais têm a possibilidade de se conectar entre si e com o mercado global. Ao permitir a transferência quase instantânea de criptomoeda, a um custo significativamente menor que os serviços estabelecidos, a blockchain torna viável economicamente a transferência de pequenas quantias de dinheiro, resultando em uma ampliação da inclusão financeira (Nordbo, 2020, p. 541).

Ao permitir que pessoas com acesso à internet ganhem dinheiro ainda armazenado em carteiras digitais, aqueles que anteriormente estavam excluídos do sistema financeiro podem ganhar e controlar seu próprio dinheiro usando Bitcoins. O uso de carteiras de Bitcoin tem o potencial de empoderar as pessoas através da propriedade de ativos e da inclusão financeira – em que pese o entendimento de Nordbo (2020). A figura a seguir traz cinco usos da criptomoeda à inclusão financeira: remessa internacional, acesso a serviços bancários, microfinanciamento, pagamento de bens e serviços e proteção contra a inflação.

Figura 4: Atividades Cotidianas de Inclusão Financeira



Fonte: Elaborado pelo Autor (2024)

Criptomoedas oferecem uma solução eficaz para as remessas internacionais, permitindo que trabalhadores estrangeiros enviem dinheiro para suas famílias em países de origem com taxas significativamente mais baixas e tempos de transferência mais rápidos do que os métodos

tradicionais. Em muitos casos, as criptomoedas eliminam a necessidade de intermediários como bancos e serviços de transferência de dinheiro, resultando em uma redução de custos e maior eficiência. Essa acessibilidade é em especial benéfica à pessoas em regiões subdesenvolvidas, onde os serviços financeiros convencionais podem ser caros ou inacessíveis (Silva, 2017).

Além das remessas, as criptomoedas estão desempenhando um papel crucial no acesso a serviços bancários. Em países onde a infraestrutura bancária é limitada, as criptomoedas permitem que pessoas sem conta bancária participem da economia digital. Com um simples smartphone e acesso à internet, indivíduos podem criar uma carteira digital, realizar transações, economizar e até investir, o que era anteriormente impossível para eles. Essa inclusão financeira ajuda o desenvolvimento econômico em comunidades desfavorecidas, permitindo escapar da pobreza e melhorar suas condições de vida (Silva, 2017).

Um outro uso relevante é o microfinanciamento. As criptomoedas facilitam a oferta de pequenos empréstimos a indivíduos ou pequenas empresas que normalmente não conseguiriam crédito através dos bancos tradicionais. Plataformas baseadas em blockchain podem oferecer microcréditos de maneira segura e transparente, sem a necessidade de uma instituição financeira intermediária. Isso é particularmente valioso em regiões onde as pessoas precisam de capital inicial para empreendimentos, mas não têm acesso a serviços bancários formais. Além disso, as criptomoedas podem ser usadas para pagar bens e serviços, tanto online quanto em lojas físicas, expandindo as opções de pagamento para aqueles que não possuem cartões de crédito ou contas bancárias (Cavalcanti, 2021).

Já, por fim, a proteção contra a inflação é um uso significativo das criptomoedas em economias instáveis. Em países onde a moeda local sofre de hiperinflação, as criptomoedas oferecem uma alternativa mais estável a preservar o valor do dinheiro. Investir em criptomoedas pode ser uma forma de proteger os ativos contra a depreciação, proporcionando uma reserva de valor mais confiável. Isso permite que indivíduos e empresas mantenham seu poder de compra em meio à instabilidade econômica, promovendo a estabilidade financeira em regiões onde as moedas fiduciárias são voláteis (Silva, 2017).

Esses cinco usos das criptomoedas para inclusão financeira demonstram seu potencial para transformar a economia brasileira. Desde facilitar remessas internacionais até fornecer acesso a serviços bancários, microfinanciamento, opções de pagamento e proteção contra a inflação, as criptomoedas estão abrindo novas oportunidades para pessoas e comunidades anteriormente excluídas do sistema financeiro tradicional

Além disso, as criptomoedas funcionam como reserva de valor para o cotidiano. Com a instabilidade econômica e a alta inflação que o Brasil enfrenta periodicamente, muitos cidadãos

e investidores buscam alternativas para preservar o valor de seus ativos. De fato, o Bitcoin, por exemplo, tem sido visto como uma forma de proteger o capital contra a desvalorização da moeda local. A terceira função é o uso de criptomoedas para remessas internacionais. O Brasil, sendo um país com uma grande diáspora, se beneficia das criptomoedas para reduzir os custos e o tempo associados às transferências de dinheiro do exterior. As criptomoedas permitem transações rápidas e baratas, eliminando a necessidade de intermediários financeiros (Bashir, 2018; Antonopoulos, 2014)

Não por menos, conforme já apresentado, as criptomoedas também têm sido utilizadas como ferramenta de crowdfunding e financiamento coletivo. Projetos e startups no Brasil estão aproveitando as *Initial Coin Offerings* (ICOs) e outras formas de captação de recursos baseadas em blockchain para financiar suas operações. Isso democratiza o acesso ao capital e impulsiona a inovação no país. Por fim, a tecnologia blockchain, que sustenta as criptomoedas, está sendo explorada para aumentar a transparência e também toda a eficiência em diversos setores, como o agronegócio, a saúde e a administração pública. No agronegócio, por exemplo, a *blockchain* pode rastrear ainda a cadeia de produção, garantindo a autenticidade e a qualidade dos produtos brasileiros no mercado internacional (Correira, 2022).

3.2.2 Promoção da Economia Social Democrática no Cotidiano

A economia social propõe responder ao desafio da perda de confiança nas instituições com uma solução inovadora: a co-construção, que se baseia na força de proposta dos cidadãos, colocados em pé de igualdade com as autoridades públicas ou também privadas. No entanto, a inteligência coletiva e a cooperação não são fáceis de implementar, especialmente devido à falta de sistemas de reconhecimento e rastreabilidade da contribuição de cada um, o que pode ainda desencorajar o compartilhamento espontâneo de informações e ideias (Antonopoulos, 2014; Judmayer et al., 2017).

A tecnologia blockchain permite toda a colaboração entre os usuários e pode, portanto, constituir uma ferramenta para o surgimento da inteligência coletiva, experimentando novas práticas de inovação e contribuição compartilhadas. Ela pode gerar as novas plataformas gerais de cocriação e permitir que indivíduos se reúnam/colaborem de maneira aberta/ descentralizada, garantindo perfeita visibilidade e rastreabilidade do valor agregado por cada um, incentivando os indivíduos a inovar e compartilhar suas ideias. A descentralização consensual da confiança

que a blockchain permite reforça, assim, as capacidades de coordenação efetiva dos indivíduos (Furneaux, 2018). De fato, a blockchain contribui para "horizontalizar" o mundo, facilitando os processos de coordenação e introduzindo um espírito de compartilhamento, de mutualização das contribuições dos membros da comunidade, gerando assim uma cooperação mais natural, mais equitativa e mais motivadora. Assume Garcia-Alfaro et al. (2017) que:

> É tecnologia que permite a diferentes atores se coordenarem entre pares, podendo, portanto, levar à experimentação de novos sistemas de governança baseados em modelos mais colaborativos. Isso poderia facilitar a tarefa das estruturas da economia social, que se baseiam amplamente em parcerias. É possível agrupar e federar as atividades de diferentes estruturas sem ter que suportar o custo e a complexidade da criação de uma entidade central para governar as relações entre os atores. A blockchain pode aqui permitir assim, toda modificação das dinâmicas de competição, incentivando a colaboração, criando efeitos de rede, novas sinergias e um ambiente de trabalho mais colaborativo e também mais participativo, que se baseia na confiança compartilhada (Garcia-Alfaro et al., 2017, p. 341).

Coinsence, por exemplo, é plataforma que incentiva a colaboração entre os membros e hoje é usada no Brasil (Silva, 2022). Destina-se aos empreendedores da economia social, às empresas sociais e aos investidores, para facilitar sua conexão e trocas. Permite aos indivíduos trabalharem juntos em projetos sociais. A plataforma é baseada na blockchain e também permite que os usuários emitam sua própria moeda, para facilitar investimentos. Todavia, é importante notar que a tecnologia blockchain não é essencialmente colaborativa: ela pode ser extrativa (com fins lucrativos) e competitiva, dependendo da maneira como é construída e utilizada. Ela pode, de fato, ser apropriada por atores motivados pelo lucro e pela extração do valor produzido, em vez de pelo benefício social e interesse geral (Morgan, 2018).

É necessário, portanto, distinguir os usos da blockchain com base em vários critérios, principalmente na finalidade e na maneira como o valor criado é redistribuído. Os princípios e regras de funcionamento das organizações da economia social são, por essência, democráticos, não estando o poder decisório atrelado à quantidade de capital detido. Em contrapartida, toda a implementação de processos democráticos e participativos pode, às vezes, revelar-se complexa. Aqui novamente, a blockchain se mostra ferramenta inovadora e também adequada. A questão fundamental reside em sua capacidade de descentralizar o consenso e a confiança entre os atores, dois temas centrais para a governança de qualquer sistema (Gates, 2017).

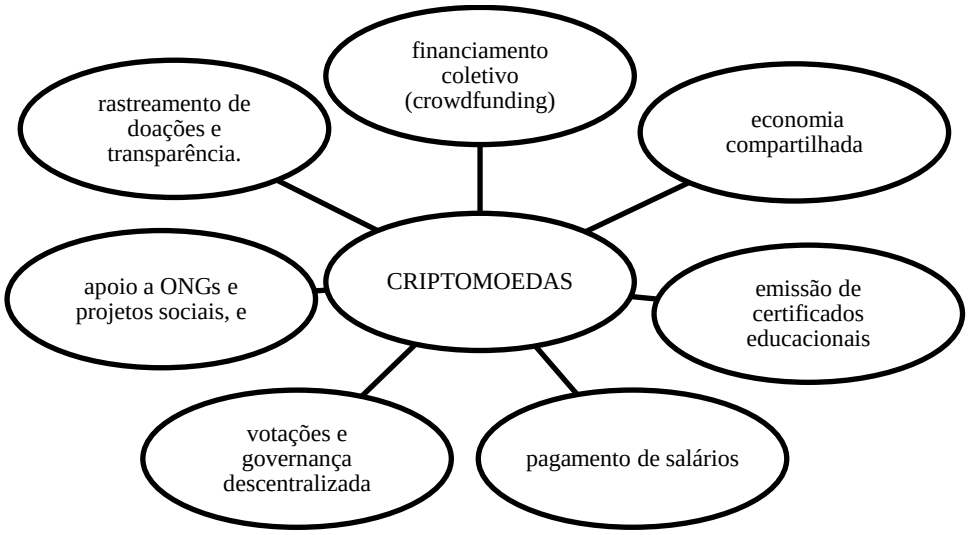
De fato, seu funcionamento carrega a promessa de um novo modelo de governança, que não se baseia em uma estrutura hierárquica rígida e fixa, mas sim em um sistema mais dinâmico e fluido. Graças à blockchain, as regras de governança podem ser automaticamente aplicadas e não podem mais ser modificadas ou contornadas. Qualquer pessoa com acesso à blockchain

pode examinar o histórico para avaliar a legitimidade das ações e das decisões realizadas pela organização. O seu registro imutável e compartilhado de transações permite a transparência e a verificabilidade, trazendo assim um grande valor em termos de responsabilidade. Isso garante uma governança mais transparente e responsável, essencial para as organizações da economia social (Isaacs, 2017).

Entre os princípios organizacionais democráticos sobre quais se baseiam organizações da economia social estão a adesão voluntária e aberta e o controle democrático pelos membros. A blockchain oferece aqui uma grande flexibilidade que responde a esses dois princípios. As exigências em termos de gestão de identidade, patrocínio de membros, supervisão social e acompanhamento podem ser construídas de maneira transparente em uma blockchain para fins de verificação e segurança. Ela também permite ainda implementar o princípio de decisão por consenso, oferecendo múltiplos procedimentos de consenso (Girasa, 2018).

Da mesma forma, a tecnologia blockchain devolve aos membros o seu lugar na tomada de decisões: a informação é verificável por todos. A tecnologia, assim, se baseia inteiramente nos usuários e lhes devolve o controle. A blockchain, como um registro distribuído, permite que uma comunidade de membros se auto-organize de maneira responsável e transparente, e facilita os procedimentos administrativos e de contabilidade, o que corresponde ainda perfeitamente às necessidades das organizações da economia social (Matharu, 2018; Garcia-Alfaro et al., 2018), fundamentalmente. Nesse horizonte, a literatura brasileira apresente sete aplicações cotidianas que estão associadas com à economia social democrática (Figura 5).

Figura 5: Atividades Cotidianas de Economia Social Democrática



Fonte: Elaborado pelo Autor (2024)

Financiamento coletivo é uma das principais no Brasil pelas quais criptomoedas podem promover a economia social democrática. Por meio de plataformas de crowdfunding baseadas em blockchain, projetos podem levantar fundos de um grande número de pequenos investidores, democratizando o acesso ao capital. Isso é especialmente útil para iniciativas comunitárias e startups sociais que, de outra forma, teriam dificuldades para obter financiamento de fontes tradicionais. A transparência inerente às transações em blockchain também aumenta a confiança entre os investidores e os promotores do projeto, pois todas as contribuições e gastos podem ser monitorados publicamente (Correia, 2022; Silveira, 2021).

Atualmente, já existem várias plataformas de financiamento participativo baseadas na tecnologia blockchain. O financiamento via blockchain também resolve, de fato, todo problema da confiança na alocação real dos fundos, devido, assim, à sua transparência. A blockchain deve permitir o surgimento de mais plataformas cooperativas descentralizadas, em detrimento das plataformas capitalistas centralizadas, como Uber ou Airbnb, que servem como intermediários nas transações. Desenvolvida em código aberto, a tecnologia blockchain permite que a oferta e a demanda se encontrem sem que uma empresa privada precise obrigatoriamente desempenhar um papel nessa intermediação (Chowdhury, 2018).

Isso evita que plataformas capitalistas, cujos principais objetivos são adquirir monopólio de mercado e rendas significativas, extraiam o valor produzido pelos usuários sem qualquer redistribuição (Airbnb, a exemplo, embolsa até 15% de cada transação realizada na plataforma) e decidam sozinhas suas regras de funcionamento. Nessas plataformas digitais, que se dizem parte da economia colaborativa, o valor criado é "capturado" e deslocalizado em benefício de investidores especulativos, sem consideração pelo aporte dos usuários (Correia, 2022; Silveira, 2021; Bashir, 2020; January, 2021; Juraszek, 2020). Tais plataformas operam em um sistema P to B to P (person-to-business-to-person), onde o intermediário busca maximizar seu lucro. Em contraste, a blockchain permite criar plataformas cooperativas baseadas em um sistema P to P (person-to-person ou peer-to-peer) sem intermediários. O movimento *Platform Cooperativism*, lançado nos Estados Unidos, aposta na solidariedade e em mudança de cultura para reconectar a economia digital com os usuários e as comunidades locais. A economia colaborativa aqui tem como princípio o bem-estar das partes interessadas e busca objetivos sociais, integrando-se assim no âmbito da economia social (Kapilendo, 2017; Roos, 2020);

Logo, as principais plataformas cooperativas que são baseadas em blockchain permitem distribuir diretamente o valor entre aqueles que o criam, oferecendo uma maior recompensa e uma melhor inclusão, e dando o poder de decisão aos usuários. O objetivo é valorizar aqueles que produzem e aumentam o valor percebido ou real da plataforma, enquanto impõem uma

distribuição justa dos rendimentos que geram ou dos bens que produzem. O objetivo principal das plataformas cooperativas não é o lucro, mas o serviço prestado à comunidade, e é nisso que elas se enquadram na economia social (Kapilendo, 2017). Essas plataformas apostam, assim, no modelo cooperativo, convidando as diferentes partes interessadas (usuários, trabalhadores, prestadores de serviços, etc.) a se envolverem no financiamento e na gestão da organização. Essa abordagem assegura um funcionamento democrático, graças ao controle pelos usuários, a um design e funcionalidades adaptados às suas necessidades, uma precificação dos serviços e condições de trabalho mais alinhadas com suas expectativas (Roos, 2020).

É importante notar, entretanto, que, hoje, oportunidades que blockchain representa para a economia social ainda são muito incertas. De fato, as plataformas cooperativas baseadas em blockchain são poucas e muitas vezes permanecem em estágio de projeto. As plataformas que permitem aos cidadãos ou empreendedores criar e trocar valor sem que este seja apropriado por oligopólios ou também monopólios privados ainda não surgiram, pelo menos não de maneira reproduzível em grande escala (Roos, 2020).

A economia compartilhada é outra área onde as criptomoedas podem ter um impacto significativo. Com a possibilidade de realizar pagamentos instantâneos e seguros, plataformas de compartilhamento de bens e serviços podem operar de maneira mais eficiente e com menores custos de transação. Isso inclui hoje desde aluguel de veículos e equipamentos até serviços de hospedagem e compartilhamento de habilidades. De fato, a utilização de criptomoedas facilita a participação de mais pessoas nesses sistemas, promovendo uma distribuição mais equitativa dos recursos e ajudando a construir comunidades mais resilientes e colaborativas (Timmers, 2021; Silveira, 2021; Costa, 2022).

A emissão de certificados educacionais e outros documentos importantes também pode ser revolucionada pelo uso de criptomoedas e tecnologia blockchain. Instituições educacionais podem emitir diplomas, certificados de cursos e outras credenciais de maneira digital e segura, garantindo a autenticidade e a imutabilidade dos documentos. Isso não só simplifica o processo de verificação para empregadores e outras instituições, mas também reduz o risco de fraudes e falsificações. A democratização do acesso à educação e à validação de competências é um passo importante para a construção de uma economia social mais justa e inclusiva (Timmers, 2021; Silveira, 2021; Costa, 2022)

No contexto do pagamento de salários, as criptomoedas oferecem uma maneira eficiente e transparente de remunerar trabalhadores, especialmente em setores informais ou em locais com sistemas bancários pouco desenvolvidos. Empresas podem pagar seus funcionários de maneira direta, rápida e com custos reduzidos, o que é particularmente benéfico em regiões

onde as transferências bancárias são caras ou inacessíveis. Além, isso pode incluir trabalhadores freelancers e *gig workers*, que frequentemente enfrentam desafios na recepção de pagamentos (Correia, 2022; Silveira, 2021). Votações e a governança descentralizada são outras aplicações cruciais das criptomoedas na promoção da economia social democrática. Utilizando contratos inteligentes e blockchain, organizações e comunidades podem conduzir votações de maneira transparente, segura e auditável. Isso é especialmente útil para cooperativas, ONGs e grupos comunitários que buscam tomar decisões de forma inclusiva e democrática. A confiança no processo eleitoral é aumentada, pois os resultados podem ser verificados por qualquer membro da comunidade (Correia, 2022; Silveira, 2021). O apoio a ONGs e projetos sociais também se beneficia do uso das criptomoedas. Doações podem ser feitas diretamente e sem intermediários, garantindo que uma amplificada parte dos fundos chegue ao destino final. A transparência das transações em blockchain permite que doadores acompanhem uso de seus fundos, aumentando a confiança e incentivando mais doações. Além disso, projetos sociais podem utilizar tokens específicos para engajar a comunidade e recompensar contribuições voluntárias (Correia, 2022; Silveira, 2021).

Por fim, todo o rastreamento de doações e a transparência são aspectos críticos onde as criptomoedas podem fazer a diferença. As ONGs e projetos sociais frequentemente enfrentam desafios em provar o uso eficaz dos fundos recebidos. Com a tecnologia blockchain, todas as transações podem ser registradas e monitoradas publicamente, aumentando a responsabilidade e a confiança dos doadores. Isso não só melhora a eficiência das operações dessas organizações, mas também pode atrair mais apoio de indivíduos e empresas que valorizam a transparência (Correia, 2022; Silveira, 2021).

3.3 DESAFIOS DO ESTABELECIMENTO DAS CRIPTOMOEDAS NO BRASIL

Há cinco categorias principais: desafios regulatórios e/ou legais, desafios tecnológicos, desafios de infraestrutura financeira, desafios de educação e conscientização, e ainda desafios de segurança e confiabilidade (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020), fundamentalmente.

Primeiro, os desafios regulatórios e legais representam um obstáculo significativo para a adoção das criptomoedas no Brasil. A falta de uma regulamentação clara e abrangente sobre o uso e a transação de criptomoedas cria incertezas tanto a investidores quanto para empresas. As autoridades brasileiras estão ainda em processo de desenvolver um marco regulatório que equilibre a inovação com a proteção ao consumidor e a prevenção de atividades ilícitas, como

lavagem de dinheiro e financiamento ao terrorismo. A incerteza regulatória pode desincentivar o investimento e a adoção de criptomoedas, além de dificultar a operação de empresas que desejam atuar nesse mercado. Em segundo lugar, os desafios tecnológicos são uma barreira importante. A infraestrutura tecnológica necessária para suportar transações de criptomoedas de maneira eficiente e segura ainda está em desenvolvimento. As redes de blockchain, embora inovadoras, enfrentam problemas de escalabilidade, latência e consumo de energia. No Brasil, a adoção em larga escala das criptomoedas exigirá melhorias significativas nas tecnologias de blockchain para garantir que possam suportar um grande volume de transações com rapidez e segurança. Além disso, a interoperabilidade entre diferentes blockchains e sistemas financeiros tradicionais é essencial para a integração completa das criptomoedas na economia (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020).

Desafios de infraestrutura financeira constituem o terceiro grupo. O sistema financeiro brasileiro, apesar de relativamente avançado, precisa se adaptar para suportar transações de criptomoedas. Isso inclui a integração de plataformas de pagamento que aceitam criptomoedas, a criação de canais de conversão eficientes entre moedas fiduciárias e criptomoedas, e a adoção de soluções de custódia seguras. A infraestrutura atual ainda não está totalmente preparada para lidar com o aumento do volume de transações e a diversidade de criptoativos disponíveis no mercado. A falta de integração com grandes players como bancos e provedores de serviços financeiros também limita a adoção e o uso das criptomoedas no dia a dia dos brasileiros. O quarto grupo de desafios é a educação e conscientização (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020).

A compreensão do funcionamento das criptomoedas e da tecnologia blockchain ainda é limitada entre a população brasileira. Muitos potenciais usuários não possuem o conhecimento necessário para operar com segurança nesse mercado, o que pode levar a fraudes e perdas financeiras. Iniciativas de educação e treinamento são cruciais para aumentar a familiaridade e a confiança nas criptomoedas. Além disso, é importante desmistificar conceitos errôneos e fornecer informações claras e acessíveis para que as pessoas possam tomar decisões informadas sobre o uso e o investimento em criptoativos (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020), fundamentalmente.

Finalmente, os desafios de segurança e confiabilidade são uma preocupação constante. O mercado de criptomoedas tem sido alvo frequente de ataques cibernéticos, fraudes e também os esquemas de pirâmide. A segurança das transações e ainda a proteção dos ativos digitais são fundamentais para garantir a confiança dos usuários. Desenvolver e/ou implementar medidas robustas de segurança, tanto a nível de infraestrutura quanto de usuário final, é essencial para

proteger contra ameaças cibernéticas. Além disso, é necessário criar mecanismos eficazes de monitoramento e resposta a incidentes para mitigar rapidamente os danos em caso de ataques (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020). Em tempo, discorrem-se sobre algumas considerações da literatura.

3.3.1 Questão Normativa: Resistência dos Governos e de Instituições Financeiras

O obstáculo mais determinante à adoção generalizada das criptomoedas é a resistência dos governos nacionais e das instituições financeiras. De fato, é pouco provável, no momento, que renunciem ao controle sobre a política monetária interna permitindo que as criptomoedas usurpem o papel de principal meio de troca. Além disso, as criptomoedas são extremamente voláteis, uma vez que não são reguladas pelas instituições. Consequentemente, essa extrema volatilidade impede que desempenhem papel maior no sistema econômico, pois não conseguem cumprir certas funções básicas que as moedas nacionais cumprem, como servir de meio de troca confiável, unidade de conta e reserva de valor (Wray, 2018).

O valor da maioria das moedas descentralizadas é a fato altamente volátil devido ao seu tamanho de mercado relativamente pequeno (isto é, porque o preço é determinado pela oferta e demanda, é necessária uma quantia menor de dinheiro para afetar o preço de uma moeda virtual do que de uma moeda fiduciária), o que gera incerteza entre os negócios e usuários que as adotam. Até mesmo o Bitcoin, que é a mais conhecida e a mais estável, tem uma volatilidade diária média de cerca de 5%. A volatilidade pode ser minimizada limitando o tempo durante o qual o valor de um usuário é armazenado sob a forma de *tokens*, ou seja, trocando-os por uma moeda fiduciária uma vez que a transação esteja concluída. É nisso que se baseiam muitos serviços de envio de remessas internacionais em criptomoeda. Alternativamente, os stablecoins, como a criptomoeda Tether, oferecem outra solução: seu valor é indexado ainda a uma moeda fiduciária através de uma empresa que garante a troca a essa taxa (Shrivastava et al., 2020), fundamentalmente.

Outro fator determinante da resistência dos governos às criptomoedas é a incerteza do ambiente jurídico e regulamentar, que impede a ampla adoção das criptomoedas na indústria de pagamentos. À medida que as criptomoedas se desenvolvem e se difundem em escala global, torna-se imperativo para os países definirem o quadro jurídico apropriado. Por enquanto, o status legal das moedas virtuais varia consideravelmente de país para outro. A grande maioria dos países considera os criptoativos como legais (sem uma proibição de compra e venda, nem de uso para a compra de bens e serviços). Outros impuseram proibições totais ou parciais às

criptomoedas (proibição generalizada, proibição de plataformas de troca comercial, proibição de uso das criptomoedas como meio de pagamento, proibição das Ofertas Iniciais de Moeda (ICO) ou restrições relativas ao setor financeiro). Outros países que proibiam ou limitavam o uso das criptomoedas desde então relaxaram suas regulamentações e estão se orientando para a autorização de seu uso. A China, por sua vez, tornou-se ainda a primeira nação a testar uma criptomoeda nacional, emitida pelo banco central (Daskalakis & Georgitseas, 2020).

A maioria dos Estados tenta regulamentar as criptomoedas adotando medidas para que seus usuários estejam sujeitos às mesmas normas regulamentares e também de proteção dos consumidores que aqueles das moedas fiduciárias. Na ausência de um quadro jurídico claro, será provavelmente necessário se submeter às regras e políticas dos mercados financeiros convencionais. Por exemplo, se um caso de uso envolver transferências de dinheiro usando criptomoedas, será necessário se submeter aos regimes regulatórios que se aplicam aos serviços de transferência de dinheiro fiduciário, incluindo as regras de KYC (*know your customer* – conheça seu cliente) e AML (*anti-money laundering* - combate à lavagem de dinheiro), em nível fundamental propriamente dito (Vaneetvelde, 2018).

Também será necessário estar atento aos conflitos de interesse que podem surgir. De fato, dada a oferta limitada de tokens, seu valor aumenta com tempo. Imagine-se, por exemplo, uma parte interessada do setor público que esteja envolvida em decisão que poderia aumentar o valor de uma criptomoeda específica. Para evitar os conflitos de interesse, o decisor deve evitar possuir tais tokens para seu próprio benefício ou transmitir informações privilegiadas a outros investidores. Os riscos podem também ser mitigados utilizando um stablecoin atrelado a uma moeda fiduciária (Costa, 2022).

Da mesma forma, vez que a blockchain não oferece um anonimato total, preocupações sobre a privacidade dos dados são levantadas: a blockchain não pode garantir a privacidade transacional, pois os valores de todas as transações e saldos de cada chave pública são visíveis publicamente. Há mesmo possibilidade de que transações possam ser vinculadas às identidades dos usuários. Diante da obrigação de proteger a privacidade de seus clientes e do direito ao esquecimento, muitas instituições financeiras hesitam em registrar transações em um registro público e imutável. O uso de blockchains de acesso restrito pode aliviar essas preocupações, limitando o número de atores que podem acessar o registro, mas apenas até certo ponto. Embora uma grande promessa da blockchain seja a pseudonimidade, a aparência de total segurança dos dados pessoais é enganosa. É verdade que um indivíduo pode preservar sua privacidade desde que o pseudônimo não esteja vinculado à pessoa por trás dele, mas assim que a conexão é feita e uma correlação estabelecida, os dados privados podem ser revelados. Não apenas a natureza

pseudônima da maioria das blockchains pode comprometer a privacidade de um indivíduo (vinculando informações de transações e chave pública, o fluxo de transações entre usuários e carteiras pode eventualmente revelar a identidade de um usuário), como também impede que as empresas compartilhem dados proprietários de forma segura (Senna; Souza, 2023; Pérez-Solà et al., 2019).

Finalmente, como destaca a Assembleia Geral das Nações Unidas, na ausência de um quadro jurídico, é legítimo estar preocupado com o fato de que as criptomoedas são cada vez mais usadas para atividades ilícitas, especialmente em matéria de corrupção, evasão fiscal e lavagem de dinheiro. De fato, várias críticas são levantadas quanto ao grau de pseudonimato que as criptomoedas oferecem aos seus usuários, vinculando as transações a carteiras digitais em vez de identidades individuais, o que abre caminho ao uso das criptomoedas para atividades delituosas como o tráfico de drogas e armas, chantagem, lavagem de dinheiro, financiamento criminoso, etc (Cavalcanti, 2021).

O rápido crescimento dos criptoativos gera uma série de oportunidades, mas também levanta certos desafios em matéria de política fiscal. Enquanto o investimento em criptoativos representa uma base tributária potencialmente importante, esses ativos colocam desafios aos formuladores de políticas, devido à "sua ausência de controle centralizado, seu pseudonimato, as dificuldades em estimar seu valor, suas características híbridas que combinam aspectos de instrumentos financeiros com ativos intangíveis, a rápida evolução da tecnologia que os sustenta e a forma desses ativos" (Drew, 2018, p. 221).

Segundo a OCDE (2024), as criptomoedas são atraentes para os criminosos, devido à sua rapidez de circulação, disponibilidade em escala global e ainda ao potencial de ocultar seus proprietários reais que apresentam, que se somam ao caráter limitado da regulamentação e ao enfraquecimento dos intermediários financeiros estabelecidos. Alguns criminosos usam as criptomoedas para comprar ou vender bens ou serviços ilícitos na dark web. Também é possível para eles converter suas criptomoedas em dinheiro (*cashing out*), através de diferentes métodos (plataformas de troca, corretores de criptomoedas, cartões pré-pagos, etc.) (Correia, 2022), em fundamentalidade.

Os intermediários fiscais, por sua vez, facilitam a lavagem dos produtos de atividades ilegais através de um serviço de mistura de criptoativos (SMC). É um serviço pago que permite aos atores ilegais lavar seus criptoativos corruptos derivados de suas atividades delituosas, misturando-os com os criptoativos legítimos de outros usuários. Vale ainda notar que 1 usuário de criptoativos pode criar um número ilimitado de carteiras. Os atores ilegais podem, portanto, criar e usar milhares de carteiras (Xavier et al., 2024).

A título de exemplo, um serviço online suspeito de ter lavado cerca de 200 milhões de dólares em criptomoeda foi apreendido pela polícia europeia em 2020. O Bestmixer.io, uma plataforma baseada em blockchain, oferecia serviços de mistura de criptoativos gerais, ou seja, serviços que permitiam assim anonimizar transações. A investigação mostrou que muitos dos criptoativos misturados na plataforma tinham origem ou destino ilegais (para ocultar e lavar o produto de atividades delituosas) (Campbell-Verduyn, 2018).

Outro exemplo é o da rede BitClub, um esquema fraudulento que solicitava fundos de investidores em troca de ações de supostas pools de mineração de criptomoedas e os recompensava se atraíssem novos clientes. Eles fraudaram esses investidores em um total de 722 milhões de dólares. Alguns casos, embora poucos, foram detectados do uso de criptomoeda por organizações terroristas, como meio de obter recursos financeiros por meio de doações. Essas criptomoedas servem "para comprar, armazenar, transportar e eventualmente usar bens e serviços em apoio a objetivos e operações terroristas" na dark web (Campbell-Verduyn, 2018; Lantz & Cawrey, 2020).

Desde 2018, o G20 (incluindo o Brasil) tem enfatizado toda a importância de melhorar a regulamentação dos criptoativos para combater, de fato, a lavagem de dinheiro e impedir o financiamento do terrorismo. Além disso, o relatório elaborado e aprovado pelos 137 membros do Quadro Inclusivo OCDE/G20 fornece uma visão geral do tratamento fiscal das criptomoedas em diferentes jurisdições e das principais lacunas em matéria de política fiscal. Ele também destaca várias considerações para os formuladores de políticas que desejam fortalecer seus quadros jurídicos e regulamentares para tributar as criptomoedas (Lantz & Cawrey, 2020). Logo, o objetivo é promover a transparência em todas as transações que envolvem criptoativos, assegurando que os rendimentos gerados pelas trocas sejam tributados, e conceber um quadro de troca internacional de maneira que todas as jurisdições que abrigam intermediários possam participar plenamente (Lantz & Cawrey, 2020).

O desenvolvimento da tecnologia blockchain apresenta um duplo problema de inclusão: do lado dos desenvolvedores e do lado do público. De fato, é necessário tanto questionar a diversidade dos desenvolvedores e programadores que moldam a blockchain quanto considerar sua acessibilidade para o grande público. Para que essa tecnologia cumpra suas promessas em termos de governança e oportunidades para a economia social, é essencial que aqueles que a constroem sejam representativos de uma população diversificada, com necessidades e expectativas muito variadas. A tecnologia não é neutra; ela é moldada por nossas escolhas, por nossas perspectivas políticas, econômicas e culturais, nossa visão de mundo (Lantz & Cawrey, 2020). Para que a blockchain revele todo o seu potencial para a economia social, é necessário

que sua estrutura também seja inclusiva. Por isso, os desenvolvedores devem vir de diferentes origens. Aqui, a multidisciplinaridade também é importante, e o desenvolvimento da blockchain deve integrar abordagens filosóficas e sociológicas, bem como jurídicas e econômicas (Lantz & Cawrey, 2020; Campbell-Verduyn, 2018).

Do lado do público, é importante notar que a tecnologia blockchain ainda é de fato muito incompreendida. O acesso aos serviços baseados em blockchain ainda é complexo, demorado e não intuitivo a qualquer pessoa que não esteja familiarizada com ela. Os programadores são os únicos a entender o que está por trás do código da blockchain e, portanto, têm em suas mãos uma ferramenta que, por enquanto, é pouco acessível ao cidadão comum, e cujo uso em larga escala apresenta riscos democráticos (Campbell-Verduyn, 2018).

O risco de exclusão dos "incompetentes" digitais é grande. Nesse sentido, a blockchain pode aprofundar ainda mais o fosso digital já existente. Os cidadãos que não têm um acesso à internet podem não ser capazes de usufruir plenamente e diretamente dos benefícios que os avanços relacionados à blockchain oferecem em termos de fortalecimento do controle sobre seus próprios dados e transações. Trata-se, portanto, de construir uma infraestrutura adaptada ao nosso mundo moderno, inteligível para todos, o que não é o caso hoje. É preciso desenvolver a tecnologia blockchain com os usuários e não para os usuários. O papel dos cidadãos deve estar no centro da concepção de qualquer iniciativa blockchain (Campbell-Verduyn, 2018), em fundamentalidade.

3.3.2 Base Tecnológica

A tecnologia por trás das criptomoedas enfrenta uma série de desafios complexos que precisam ser superados para que essas moedas digitais possam ser adotadas em larga escala. Sete dos principais desafios tecnológicos incluem escalabilidade, interoperabilidade, consumo de energia, latência, complexidade técnica, governança descentralizada e inovação contínua, à luz da literatura (Rodrigues & Kurtz, 2019; Pérez-Solà et al., 2019; Furneaux, 2018; Edmunds, 2020; Antonopoulos, 2015; Jordan, 2020; Bashir, 2020).

1) Escalabilidade: as redes de blockchain, como a do Bitcoin e do Ethereum, enfrentam limitações significativas em termos de quantas transações podem processar por segundo. Por exemplo, o Bitcoin processa cerca de 7 transações por segundo, enquanto o Ethereum lida com aproximadamente 30. Esses números são insignificantes comparados aos sistemas tradicionais de pagamento, como Visa, que pode processar milhares de transações por segundo. Soluções como a *Lightning Network* para Bitcoin e Ethereum 2.0, que introduz a prova de participação

(*Proof of Stake*) e o *sharding*, estão sendo desenvolvidas, mas a implementação completa e/ou bem-sucedida dessas soluções ainda está em andamento (Rodrigues & Kurtz, 2019).

2) Interoperabilidade: a falta de interoperabilidade entre diferentes blockchains é outro grande desafio. Atualmente, as criptomoedas operam em suas próprias redes independentes, o que dificulta a troca direta de valor entre elas sem o uso de intermediários, como *exchanges* centralizadas. Projetos como Polkadot e Cosmos estão tentando resolver esse problema criando infraestrutura que permite a comunicação entre diferentes blockchains, mas essa tecnologia ainda está em seus estágios iniciais (Pérez-Solà et al., 2019).

3) Consumo de Energia: é um desafio significativo, especialmente para criptomoedas que utilizam o mecanismo de consenso de prova de trabalho (*Proof of Work*). Minerar Bitcoin, por exemplo, consome uma quantidade enorme de eletricidade, comparável ao consumo de energia de países inteiros. Esse alto consumo não é sustentável a longo prazo e tem levado a críticas em termos de impacto ambiental. Alternativas como a prova de participação (Proof of Stake) e outros métodos de consenso menos intensivos em energia estão sendo exploradas, mas ainda enfrentam desafios de segurança e implementação (Furneaux, 2018).

4) Latência: em muitas redes de blockchain, pode levar de alguns minutos a várias horas para que uma transação seja confirmada, o que não é viável para muitos casos de uso diário, como pagamentos em lojas. Melhorias na velocidade de confirmação direta das transações são necessárias para que as criptomoedas possam competir com sistemas de pagamento tradicionais (Edmunds, 2020).

5) Complexidade Técnica: para os desenvolvedores, criar aplicativos descentralizados (dApps) e contratos inteligentes seguros e eficientes é desafio; para os usuários, a compreensão de conceitos básicos de blockchain, gestão de chaves privadas e segurança de criptomoedas pode ser extremamente complicada. Ferramentas e interfaces de usuário mais amigáveis são necessárias para aumentar a adoção (Antonopoulos, 2015; Jordan, 2020).

6) Governança Descentralizada: decisões sobre atualizações de rede, resolução de *bugs* e outras questões de governança são tomadas através por meio de processos descentralizados, como votações entre os detentores de tokens, que podem ser lentos e sujeitos a disputas, o que pode atrasar melhorias e respostas a problemas críticos. A criação de modelos de governança mais eficientes e justos é uma área de pesquisa ativa (Jordan, 2020; Bashir, 2020).

7) Inovação Contínua: o ritmo rápido de inovação no espaço das criptomoedas é tanto uma força quanto um desafio, pois as novas tecnologias, algoritmos de consenso, e padrões de criptografia estão sendo constantemente desenvolvidos e, assim, manter-se atualizado com tais inovações e integrá-las de maneira segura nas redes existentes é um desafio constante para os

desenvolvedores. Além disso, a inovação rápida pode levar a um ambiente fragmentado, onde diferentes plataformas e tecnologias não são compatíveis umas com as outras, dificultando a criação de um ecossistema coeso (Bashir, 2020). Esses desafios são interconectados e muitas vezes exigem soluções complexas e colaborativas para serem superados.

3.3.3 Segurança e Infraestrutura

A segurança e também infraestrutura das criptomoedas são fundamentais para garantir a confiança dos usuários e a estabilidade do sistema. Os quatro desafios principais nessa área incluem segurança das carteiras, ataques cibernéticos, a integridade dos contratos inteligentes, robustez da rede e a resiliência a ataques (Hosp, 2017; Nordbo, 2020; Raymond, 2020; Wray, 2018; Shrivastava et al., 2020; Daskalakis & Georgitseas, 2020).

A) Segurança das Carteiras: a segurança das carteiras digitais onde as criptomoedas são armazenadas é um desafio crítico, pois os usuários precisam proteger suas chaves privadas para evitar a perda de fundos. As carteiras digitais podem ser vulneráveis a ataques de malware, phishing e outras formas de hacking. Soluções de hardware, como carteiras frias (*cold wallets*), oferecem maior segurança, mas podem ser menos convenientes para transações diárias. A educação dos usuários sobre práticas seguras de armazenamento de criptomoedas é essencial para mitigar esses riscos (Hosp, 2017).

B) Ataques Cibernéticos: *hackers* podem explorar vulnerabilidades para roubar grandes quantidades de criptomoedas, como foi o caso dos notórios ataques às exchanges Mt. Gox e Coincheck. Garantir segurança de *exchanges* e plataformas através de medidas como auditorias de segurança regulares, testes de penetração e protocolos de segurança robustos é crucial para proteger os ativos dos usuários (Raymond, 2020; Wray, 2018).

C) Integridade dos Contratos Inteligentes: contratos inteligentes são uma característica fundamental de muitas plataformas de blockchain, permitindo, de fato, a execução automática de acordos quando certas condições são atendidas. No entanto, a segurança desses contratos depende da qualidade do código, e bugs ou também vulnerabilidades podem ser explorados por atacantes. Auditorias de código e padrões de desenvolvimento rigorosos são necessários para garantir que todos os contratos inteligentes sejam seguros e confiáveis (Shrivastava et al., 2020; Daskalakis & Georgitseas, 2020).

D) Robustez da Rede: a robustez das redes de blockchain é crucial para a segurança e estabilidade das criptomoedas. Ataques tais como o de negação de serviço distribuído (DDoS) podem sobrecarregar a rede e interromper o funcionamento normal. Protocolos de segurança,

como a implementação de sistemas de detecção e mitigação de DDoS, são essenciais para manter a integridade da rede. Além disso, a redundância e a descentralização da infraestrutura podem aumentar a resiliência da rede (Hosp, 2017). Tão logo, garantir a segurança das carteiras e das exchanges, regular de forma eficaz o mercado, proteger contra fraudes, assegurar a integridade dos contratos inteligentes, aumentar a robustez da rede e desenvolver defesas contra ataques de 51% são passos essenciais para criar um ambiente seguro e ainda confiável para os usuários de criptomoedas.

3.3.4 Educação e Confiabilidade

Três desafios principais nessa área incluem alfabetização digital, desinformação e a transparência das operações (Vaneetvelde, 2018; Costa, 2022; Senna; Souza, 2023; Pérez-Solà et al., 2019; Cavalcanti, 2021; Silva, 2021; Correia, 2022; Xavier et al., 2024). Estas são, assim, discorridas a seguir.

1) Alfabetização Digital: é um desafio significativo, especialmente em países onde o acesso à tecnologia e à internet ainda é limitado. Muitos indivíduos ainda não têm as habilidades necessárias para entender e utilizar criptomoedas de forma segura. Iniciativas para melhorar a alfabetização digital são essenciais para capacitar mais pessoas a participar do ecossistema de criptomoedas. Programas educacionais voltados para ensinar os fundamentos da tecnologia blockchain, criptomoedas e segurança digital podem ajudar a reduzir as barreiras de entrada e aumentar a confiança dos usuários (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020), fundamentalmente.

2) Desinformação: as informações incorretas ou enganosas podem levar a decisões de investimento ruins e aumentar a desconfiança no mercado. As campanhas de conscientização e fontes confiáveis de informação são essenciais para combater a desinformação. Instituições educacionais e organizações do setor podem desempenhar, assim, amplo papel importante na disseminação de informações precisas e atualizadas sobre criptomoedas (Matos et al., 2021; Xavier et al., 2024; Wray, 2018; Olívia et al., 2020).

3) Transparência das Operações: os usuários precisam ter visibilidade sobre como suas criptomoedas são gerenciadas, como as transações são processadas e como as medidas de segurança são implementadas. Publicar relatórios regulares e detalhes sob práticas operacionais pode aumentar a transparência e confiança (Matos et al., 2021; Xavier et al., 2024). Abordar esses desafios permitirá que mais pessoas se beneficiem das oportunidades oferecidas pelas criptomoedas, promovendo uma maior inclusão financeira e tecnológica (Matos et al., 2021).

4 CONSIDERAÇÕES FINAIS

Em conclusão, a adoção das criptomoedas no cotidiano apresenta um panorama repleto de potencialidades e desafios complexos. As criptomoedas têm demonstrado gama diversificada de aplicações práticas que podem revolucionar a economia global e transformar o cotidiano das pessoas. Entre os principais usos, destacam-se: pagamentos P2P, a transferência internacional de remessas, a facilitação de microtransações, o uso como uma reserva de valor, a aplicação em contratos inteligentes, a tokenização de ativos, a execução de operações no mercado financeiro, a utilização em programas de fidelidade, a compra e venda de bens e serviços online e offline, a doação a causas sociais, a recompensação de criadores de conteúdo, a implementação em jogos digitais, a integração em sistemas de pagamento de transporte público, o financiamento coletivo (crowdfunding) e emissão de identidades digitais.

Todavia, a concretização plena dessas potencialidades esbarra em uma série de desafios substanciais que demandam atenção e resolução. Entre os obstáculos mais significativos estão a escalabilidade das redes blockchain, que precisa ser aprimorada para lidar com um volume crescente de transações; a interoperabilidade entre diferentes plataformas de criptomoedas, que ainda é limitada; a volatilidade dos preços das criptomoedas, que dificulta sua aceitação como meio de pagamento estável; a complexidade técnica das plataformas, que pode ser um entrave para usuários leigos; a regulamentação fragmentada e inconsistente, que gera ainda incertezas jurídicas; a vulnerabilidade aos ataques cibernéticos, fraudes e roubos, que ainda preocupam investidores e usuários; a necessidade de uma infraestrutura tecnológica robusta, especialmente em áreas menos desenvolvidas; a falta de programas educativos que possam aumentar o conhecimento e a confiança do público em relação às criptomoedas; a resistência cultural e institucional à mudança, que pode retardar a adoção; e a questão da sustentabilidade ambiental, especialmente no que tange ao consumo energético dos processos de mineração.

Portanto, a pesquisa sobre os desafios e perspectivas para a adoção das criptomoedas no cotidiano revela um campo repleto de oportunidades, mas também de dificuldades que exigem abordagens inovadoras e colaborativas. Em tempo, toda a superação desses desafios demanda uma convergência de esforços de diversos atores, incluindo governos, instituições financeiras, empresas de tecnologia e a sociedade civil. A implementação de políticas regulatórias claras e consistentes, o desenvolvimento de soluções tecnológicas que aumentem a segurança e a usabilidade, a construção de uma infraestrutura tecnológica inclusiva e acessível, e a promoção de programas educacionais abrangentes são passos essenciais para criar um ambiente favorável à adoção das criptomoedas, fundamentalmente.

Somente através de um esforço coordenado e multidisciplinar será possível transformar as criptomoedas de um nicho tecnológico em ferramenta amplamente utilizada, promovendo uma economia mais inclusiva, transparente e eficiente. A potencialidade das criptomoedas de facilitar transações seguras, rápidas e de baixo custo, junto com a capacidade de descentralizar o poder financeiro, oferece caminho promissor para o futuro das finanças globais. No entanto, é imperativo enfrentar e mitigar desafios existentes para alcançar uma adoção significativa e sustentável, garantindo que benefícios das criptomoedas possam ser plenamente realizados e amplamente distribuídos na sociedade.

Quanto aos estudos futuros, em primeiro lugar, deve-se investigar toda a evolução das regulamentações globais e também o seu impacto na adoção e na utilização das criptomoedas. Compreender como diferentes abordagens regulatórias influenciam a percepção de segurança e a confiança dos usuários pode trazer dados sobre como criar um ambiente regulatório favorável e consistente, especialmente em relação à segurança. Além disso, explorar novas tecnologias e protocolos para melhorar a escalabilidade das redes blockchain é um segundo eixo essencial. A capacidade de processar um maior volume de transações de forma eficiente e econômica é fundamental para viabilizar o uso das criptomoedas em escala global, especialmente em face do crescimento contínuo da demanda. Por fim, um terceiro eixo promissor envolve investigar estratégias para aumentar a interoperabilidade entre diferentes plataformas de criptomoedas. Atualmente, a limitada interoperabilidade pode dificultar a integração e a utilização eficiente das criptomoedas em diversos contextos. Pesquisas focadas, assim, em desenvolver protocolos e soluções que permitam uma colaboração mais fluida entre ecossistemas cripto podem acelerar a adoção e expandir as possibilidades de aplicação dessas tecnologias inovadoras.

REFERÊNCIAS

ANTONOPOULOS, A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [1 ed.]. Sebastopol: O'Reilly Media, 2014.

ANTONOPOULOS, A. M. Mastering Bitcoin: Unlocking Digital Cryptocurrencies [First ed.]. Sebastopol: O'Reilly Media, 2015.

BASHIR, I. Mastering Blockchain: A Deep Dive into Distributed Ledgers, Consensus Protocols, Smart Contracts, DApps, Cryptocurrencies, Ethereum, and More [3 ed.]. Birmingham: Packt Publishing, 2020.

BASHIR, I. Mastering Blockchain: A Deep Dive into Distributed Ledgers, Consensus Protocols, Smart Contracts, DApps, Cryptocurrencies, Ethereum, and More [3 ed.]. 2020.

CAMPBELL-VERDUYN, M. (Ed.). Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance [1st ed.]. London: Routledge/Taylor & Francis Group, 2018.

CAVALCANTI, T. R. Confiança no mercado de criptomoeda. Tese. (doutorado) — Universidade de Brasília, Faculdade de Administração, Contabilidade, Economia e Gestão de Políticas Públicas, Departamento de Economia, Brasília, 2021.

CHOWDHURY, N. Inside Blockchain, Bitcoin, and Cryptocurrencies. Boca Raton: CRC Press, 2018.

CORREIA, L. C. Fatores de influência na compra de criptomoedas no Brasil. Universidade Federal de Juiz de Fora (UFJF) Programa de Pós-Graduação, Mestrado Acadêmico em Administração, Faculdade de Administração e Ciências Contábeis, 2022

COSTA, F. R. Juridicização dos criptoativos: a natureza jurídica das criptomoedas e dos contratos inteligentes. Universidade Federal de Juiz de Fora (UFJF). Programa de Pós-graduação em Direito e Inovação, Faculdade de Direito, 2022

DASKALAKIS, N.; GEORGITSEAS, P. An Introduction to Cryptocurrencies: The Crypto Market Ecosystem. New York: Routledge, 2020.

DUPONT, Q. Cryptocurrencies and Blockchains. Cambridge: Polity Press, 2019.

EDMUNDS, J. C. Rogue Money and the Underground Economy: An Encyclopedia of Alternative and Cryptocurrencies. Santa Barbara: ABC-CLIO, 2020.

FERREIRA, Natasha Alves. Incertezas jurídicas e econômicas da Bitcoin como moeda. 27 f. Dissertação (Especialização em Direito), IMED - Faculdade Meridional, 2014.

FURNEAUX, N. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence [1 ed.]. Hoboken: Wiley, 2018.

FURNEAUX, N. Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence. 2018.

GARCIA-ALFARO, J.; HERRERA-JOANCOMARTÍ, J.; LIVRAGA, G.; RIOS, R. Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2018 International Workshops, DPM 2018 and CBT 2018, Barcelona, Spain, September 6-7, 2018, Proceedings [1st ed.]. Cham: Springer International Publishing, 2018.

GAREWAL, K. S. Practical Blockchains and Cryptocurrencies: Speed Up Your Application Development Process and Develop Distributed Applications with Confidence [1st ed.]. New York: Apress, 2020.

GATES, M. Blockchain: Ultimate Guide to Understanding Blockchain, Bitcoin, Cryptocurrencies, Smart Contracts and the Future of Money. North Charleston: CreateSpace Independent Publishing Platform, 2017.

GIRASA, R. Regulation of Cryptocurrencies and Blockchain Technologies [1st ed.]. Cham: Springer International Publishing; Palgrave Macmillan, 2018.

GRABOWSKI, M. Cryptocurrencies: A Primer on Digital Money. New York: Routledge, 2019. ISBN 9780429201479. Pdf.

HOSP, J. Cryptocurrencies Simply Explained: By TenX Co-Founder Dr. Julian Hosp: Bitcoin, Ethereum, Blockchain, ICOs, Decentralization, Mining & Co. Hong Kong: Dr. Julian Hosp; Lightning Source, 2017.

ISAACS, J. Bitcoin: A Step-by-Step Guide on Mastering Bitcoin and Cryptocurrencies. North Charleston: CreateSpace Independent Publishing Platform, 2017.

JANUARY, B. Cryptocurrencies and the Blockchain Revolution: Bitcoin and Beyond. Minneapolis: Lerner Publishing Group, 2021.

JORDAN, S. How to Make Money with Stocks Online: 3 Books in 1: The Complete Beginners' Guide for Learning How to Trade Options, Swing Trading Strategies and Bitcoin Cryptocurrencies Online Trading. 2020.

JUDMAYER, A.; STIFTER, N.; KROMBHOLZ, K.; WEIPPL, E. Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies and their Consensus Mechanisms. San Rafael: Morgan & Claypool, 2017.

JURASZEK, A. Cryptocurrency and Blockchains Explained [1st ed.]. New York: Adams Media, 2020.

KAPILENDO. The Cryptocurrencies That Matter. Berlin: Kapilendo AG, 2017.

LANTZ, L.; CAWREY, D. Mastering Blockchain: Unlocking the Power of Cryptocurrencies, Smart Contracts, and Decentralized Applications. Sebastopol: O'Reilly Media, 2020. 284 p.

LEWIS, A. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Coral Gables: Mango Publishing Group, 2018. 408 p.

LEWIS, A. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them. Coral Gables: Mango Media; Mango Publishing, 2023.

MATHARU, A. Understanding Cryptocurrencies. New York: Business Expert Press, 2018.

MATTOS, O. B., et al. As criptomoedas e os novos desafios ao sistema monetário: uma abordagem pós-keynesiana. Economia E Sociedade, v. 29, n. 3, p. 761–778, 2020.

MATTOS, S. et al. As criptomoedas e os novos desafios ao sistema monetário: uma abordagem pós-keynesiana. Econ. soc., 29, n. 3, 2020

MENEGATTI, M. et al. Decisão de Compras Pela Internet: Uma Análise a Partir do Tempo de Utilização de Mídias Sociais e da Interatividade com a Marca. Revista Brasileira de Marketing., v. 16, n. 1, p. 41-54, 2017

MORGAN, J. P. Decrypting Cryptocurrencies: Technology, Applications and Challenges. 2018.

NORDBO, L. Top 100 Cryptocurrencies: Mastering Cryptocurrencies. 2020. Epub.

PÉREZ-SOLÀ, C.; NAVARRO-ARRIBAS, G.; BIRYUKOV, A.; GARCIA-ALFARO, J. Data Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 and CBT 2019, Luxembourg, September 26-27, 2019, Proceedings [1st ed. 2019]. Cham: Springer International Publishing, 2019.

RAJ, K. Foundations of Blockchain: The Pathway to Cryptocurrencies and Decentralized Blockchain Applications. Birmingham: Packt Publishing, 2019.

RAYMOND, D. Stock Market Investing for Beginners: 6 Books in 1: Best Strategies and Tactics for Building Income by Trading Stocks, Bonds, Options, Forex, Cryptocurrencies, and More. 2020

RODRIGUES, G.; KURTZ, L. Cryptocurrencies and Anti-Money Laundering Regulation in the G20. Belo Horizonte: Institute for Research on Internet and Society - IRIS, 2019.

ROOS, S. W. Cryptocurrency and Blockchain Technology: The Complete Guide to Understanding Cryptocurrency, Blockchain, Mining, Trading, ICOs, Ethereum Platform, and the Bitcoin Revolution. 2022

SENNA V de, SOUZA AM. Criptomoedas e sistema financeiro: revisão sistemática de literatura. Rev adm empres [Internet], e2145, p. 2022–0019, 2023

SHRIVASTAVA, G.; LE, D.-N.; SHARMA, K. (Eds.). Cryptocurrencies and Blockchain Technology Applications. Hoboken: John Wiley & Sons Inc, 2020.

SILVA, A. T. As criptomoedas como expressões endêmicas do ciberespaço. Universidade Federal de Mato Grosso, Faculdade de Comunicação e Artes (FCA) UFMT CUC – Cuiabá, Programa de Pós-Graduação em Estudos de Cultura Contemporânea, 2021.

SILVA, Daniel Carmo Da. Contabilidade na era digital: um estudo sobre o reconhecimento contábil das transações realizadas com Bitcoins no Brasil. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis). Centro Universitário de Brasília, Brasília, 2017. P 79.

SILVEIRA, L. M. Desmistificando as criptomoedas: a contribuição das moedas virtuais na diversificação dos investimentos. Universidade Federal de Santa Maria, Centro de Ciências Sociais e Humanas, Programa de Pós-Graduação em Administração, 2021

STATISTA. Statista Plataform: Brazil – Cripto. Statista (online), 2024.

TAPSCOTT, D.; TAPSCOTT, A. Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World [Reprint ed.]. New York: Penguin Publishing Group, 2018.

TIMMERS, M. J. S. Criptomoedas e o comportamento do investido: um estudo a partir da cultura política. Rev. Economia, v. 1, n. 13, 2018,

TIMOTIO, G. et al. Inclusão financeira no brasil: investigação a partir da construção de indicadores. Congress USP, VXIII, PP. 405-455, 2018

VAN DER AUWERA, E.; SCHOUTENS, W.; GIUDICI, M. P.; ALESSI, L. Financial Risk Management for Cryptocurrencies [1st ed.]. Cham: Springer International Publishing; Springer, 2020.

VAN FLYMEN, D. Learn Blockchain by Building One: A Concise Path to Understanding Cryptocurrencies [1st ed.]. New York: Apress, 2020. 1

VANEETVELDE, K. Ethereum Projects for Beginners: Build Blockchain-Based Cryptocurrencies, Smart Contracts, and DApps [1 ed.]. Birmingham: Packt Publishing, 2018.

WEF. World Economic Forum. All you need to know about blockchain, explained Simply. WEF Blog (online), 16 de junho. 2016. Disponível em: https://www.weforum.org/agenda/2016/06/blockchain-explained-simply/. Acesso em 04 jun. 2024.

WRAY, L. R. Trabalho e moeda hoje: a chave para o pleno emprego e a estabilidade de preços. Rio de Janeiro: Editora UFRJ/Contraponto, 2018.

XAVIER, M. et al. Criptomoedas: seus desafios de regulamentação e os impactos a instituições financeiras centralizadas. International Journal of Professional Business Review., v. 9., n. 1, fev/2014