Um Estudo Econômico-Computacional Aplicado Sobre Criptoativos

An Applied Economic-Computational Study On Cryptoassets

Heber José da Silva Junior[1]
Mario Henrique Akihiko da Costa Adaniya[2]

Resumo

Nos últimos anos, as criptomoedas têm conquistado seu caminho no cenário financeiro global, trazendo uma nova maneira na realização de transações econômicas. A ascensão das moedas digitais como o *Bitcoin* e *Ethereum* trouxeram consigo não apenas uma revolução na tecnologia financeira, mas também uma onda de especulação, debate e inovação. No entanto, além do seu potencial como veículo de investimento e meio de troca, o mundo dos criptoativos abre portas também para a propósitos educacionais. Este artigo explora a possibilidade e a tecnologia necessária no desenvolvimento de um criptoativo educacional, voltado a refinar a maneira em que as pessoas aprendem os princípios fundamentais da ciência econômica e financeira. Este projeto se utiliza das bases das moedas digitais, suas tecnologias empregadas e seu impacto sobre a economia tradicional, se apoiando também na definição do dinheiro sob a visão dos autores presentes na Escola Austríaca de Economia.

Palavras-chave: Tecnologia financeira; Economia; *Blockchain*; *Bitcoin*; Educação financeira; Criptoativos; *DeFi*.

Abstract

In recent years, cryptocurrencies have burst onto the global financial scene, bringing with them a new way of conducting economic transactions. The rise of digital currencies such as bitcoin and ethereum has not only revolutionized financial technology, but also sparked a wave of speculation, debate, and innovation. But beyond its potential as an investment vehicle and medium of exchange, the world of cryptoassets also opens doors for educational purposes. This article explores the possibility and the technology required to develop an educational cryptoasset aimed at refining the way people learn the basic principles of economics and finance. This project uses the fundamentals of digital currencies, their technologies and their impact on the traditional economy, and also draws on the definition of money from the point of view of the authors of the Austrian School of Economics.

Keywords: Financial technology; Economics; *Blockchain*; *Bitcoin*; Financial education; Cryptoassets; *DeFi*

INTRODUÇÃO

Os criptoativos, também conhecidos como criptomoedas ou moedas digitais, são representações digitais de valor que utilizam criptografia para garantir transações seguras e controlar a criação de novas unidades (YETMAR, 2023). Ao contrário das moedas governamentais tradicionais, os criptoativos operam em redes descentralizadas, geralmente baseadas em tecnologia de *Blockchain*, onde a validação das transações é realizada pelos próprios participantes da rede através de um consenso distri-

[1]Centro Universitário Filadélfia de Londrina - UniFil
[2]Centro Universitário Filadélfia de Londrina - UniFil

buído. Este ambiente transparente, seguro e descentralizado existe graças a arquiteturas de *software* complexas e dedicadas ao propósito de escalabilidade, segurança e autonomia do ativo. Diante da versatilidade dos criptoativos, este projeto de pesquisa visa esclarecer o entendimento popular dos criptoativos enquanto expõe uma análise técnica e econômica do mesmo.

Na seção utilizamos do *Bitcoin* como exemplo, expomos o contexto de aplicação deste ativo, seu posicionamento sobre o dinheiro tradicional e como podemos utilizar do ambiente das criptos para buscar independência monetária. É apresentado também a tecnologia de encadeamento e rede em que o Bitcoin atua — a *Blockchain*, a tecnologia Prova de Trabalho, ou *Proof of work*, utilizada como validador de novos blocos e a técnica utilizada na assinatura de transações dentro da *Blockchain* — a criptografia de chave pública e privada.

Pela seção são adotadas as definições de dinheiro, economia e capital da Escola Austríaca de Economia. Será utilizado dos conceitos financeiros para definir quão bem o criptoativo consegue servir as atividades econômicas.

Durante a seção é feita uma revisão do livro "*Bitcoin*, A Moeda Na Era Digital" do mestre brasileiro em economia Fernando Ulrich. Neste livro o autor também revisa o posicionamento da Escola Austríaca de Economia diante do conceito de dinheiro e moeda, traz contexto histórico sobre o desenvolvimento do *Bitcoin* e defende a utilização do criptoativo como moeda de troca legítimo.

Por fim, no capítulo **??**, propomos a ideia do desenvolvimento de uma criptomoeda capaz de conteinerizar e abstrair os conceitos básicos do ensino de economia, provendo autonomia para professores simularem ambientes econômicos. Assim demonstrando e aplicando o conhecimento teórico da ciência financeira.

Embora as criptomoedas tenham ganhado destaque, a compreensão abrangente de seu estado técnico atual permanece fragmentada. Esta falta de clareza popular diante do contexto de criptoativos torna o conceito menos palatável à aceitação pública da tecnologia. Embora compreendível a baixa adesão popular a tal tecnologia, é possível estipular melhorias de qualidade de vida diante da população passando despercebidas.

Como conceito, as finanças descentralizadas nasceram visando denunciar as consequências sofridas pela população devido ao mal uso governamental do curso forçado das suas respectivas moedas. A ideia de retirar a manipulação central do

dinheiro cria impeditivos físicos ao ativo de sofrer anomalias econômicas como a inflação, por exemplo, visto que o comportamento de escassez da moeda é absoluto (no caso do *Bitcoin*).

Conforme o mestre em desenvolvimento econômico Pedro Lopes Marinho, em 2001, devido o início da Primeira Guerra Mundial, o sistema monetário padrão-ouro foi mundialmente abolido enquanto governos financiavam os gastos militares a partir da emissão de moedas. Uma vez que o lastro em metal na moeda foi abandonado, o maior impeditivo a impressão deliberada de dinheiro — e posteriormente inflação — foi deixado de lado.

A ideia da economia estar sob o controle absoluto governamental implica que todo o trabalho, tempo, esforço e riqueza de uma população está a uma ordem de distância de ser descartada por mal uso estatal da sua moeda.

Assim que as finanças descentralizadas tomam seu devido foco. Uma vez oferecendo independência, autonomia, transparência e integridade dos seus protocolos, as moedas digitais podem garantir que o poder e a responsabilidade do dinheiro estão apenas sob quem os detém, seguindo a máxima popular do ambiente cripto “Minhas chaves, minhas moedas”.

O projeto de pesquisa passa pela limitação de que, no estado atual de atividade entre meio destes ativos, o lançamento de novas moedas digitais são extremamente frequentes, gerando constante necessidade de reindexação da funcionalidade e atuação de cada nova moeda.

METODOLOGIA DE PESQUISA

A pesquisa foi conduzida inicialmente através de uma extensa revisão sistemática da literatura, diante das revistas acadêmicas ACM, *Semantic Scholar*, IEEE, em busca de artigos apresentando o estado da arte na área de criptoativos. Foram coletados 86 artigos selecionados inicialmente pelas palavras chaves Criptoativos, *Bitcoin*, *Smart Contracts*, *Blockchain*, *DeFi* e *Web 3*. Utilizamos a revisão destes artigos de modo a buscar o estado da arte documentado diante dos criptoativos.

Após a coleta inicial dos artigos, o primeiro processo de filtragem se passou pela leitura do resumo dos artigos, mantendo apenas os documentos que retratavam a utilização e o impacto socio-econômico dos criptoativos e a exploração do conceito

de finanças descentralizadas. Esta primeira filtragem nos retornou 58 registros.

O segundo processo de filtragem passou-se pela leitura do conteúdo de cada artigo, buscando apenas os relacionamentos dentre os termos técnicos de economia paralelamente ao funcionamento dos ativos digitais. Diante deste processamento de documentação, foi constatada a necessidade da busca bibliográfica de referências da Escola Austríaca de Economia — devido à semelhança de comportamento agnóstico ao estado tanto desta vertente acadêmica quanto das finanças descentralizadas — no que foi considerada busca de literatura de seus principais autores. Esta segunda filtragem nos retornou 7 livros e 27 artigos.

Por fim, a partir da leitura de toda a documentação coletada, foi registrado o estado da arte na utilização de criptoativos, dentre seus serviços, propostas e ferramentas. Foi registrada também a atuação técnica da moeda digital mais utilizada atualmente, o *Bitcoin*[1], registrado o comportamento do ativo diante da visão da Escola Austríaca de Economia e documentado as comparações dos ativos digitais diante do ouro e o papel-moeda.

FUNDAMENTAÇÃO TEORICA

O estudo dos criptoativos, frequentemente referidos como criptomoedas, emergiu como uma área interdisciplinar que engloba finanças, economia, ciência da computação, direito e outras disciplinas correlatas. O estado da arte nesta área é caracterizado por avanços tecnológicos inovadores, desafios regulatórios complexos, crescente adoção institucional e individual, e um cenário de rápida evolução e inovações contínuas. A seguir constam as principais tecnologias aplicadas ao ambiente das finanças distribuídas brevemente descritas.

Blockchain e Tecnologia de Registro Distribuído (DLT)

A *blockchain*, a partir da Tecnologia de Registro Distribuído (DLT, do inglês - *Distributed Ledger Technology*), é o alicerce sobre o qual a maioria dos criptoativos é construída. Sua estrutura descentralizada permite a verificação e registro de transações por uma rede distribuída de nós, assegura características fundamentais como imutabilidade, transparência e resistência à censura (NAKAMOTO, 2009). Além disso,

[1] Conforme o indexador de criptoativos *CoinGecko*, acessado 22/05/2024

protocolos de consenso como *Proof of Work (PoW)* e *Proof of Stake (PoS)* são cruciais para a segurança e eficiência das redes *blockchain*.

Contratos Inteligentes

Contratos inteligentes *(smart contracts)* são programas autoexecutáveis que operam quando condições predefinidas são atendidas. Introduzidos pela plataforma *Ethereum* (BUTERIN, 2013), esses contratos têm o potencial de automatizar e desintermediar uma vasta gama de transações e processos contratuais, desde serviços financeiros até cadeias de suprimentos. A segurança e a flexibilidade proporcionadas pelos contratos inteligentes incentivam a criação de Aplicações Descentralizadas, que operam em redes *blockchain* sem necessidade de intermediários confiáveis.

Interoperabilidade

Um dos desafios técnicos significativos é a interoperabilidade entre diferentes blockchains. Projetos como *Polkadot* (WOOD, 2016) e Cosmos (KWON, 2016) estão na vanguarda do desenvolvimento de soluções que permitem a comunicação e a interação entre diversas redes *blockchain*. Esta interoperabilidade é essencial para a criação de um ecossistema de criptoativos mais integrado e funcional, onde ativos e informações podem ser transferidos de maneira segura e eficiente entre diferentes plataformas.

Adoção Pública aos Criptoativos

Panorama Governamental - O cenário regulatório dos criptoativos é altamente diversificado e dinâmico. Países como Suíça e Singapura têm adotado abordagens regulatórias favoráveis, criando ambientes propícios para inovação e atração de investimentos (ZOHAR, 2015). Em contraste, nações como China e Índia têm implementado restrições rigorosas ao uso e comércio de criptoativos, citando preocupações com a estabilidade financeira e a proteção ao consumidor (AUER; CLAESSENS, 2018).

Instituições internacionais, como o *Financial Action Task Force (FATF)*, estão desenvolvendo diretrizes para mitigar os riscos associados aos criptoativos, como a lavagem de dinheiro e o financiamento do terrorismo (FATF, 2019). A União Europeia,

com sua proposta de Regulamento de Mercados de Criptoativos (MiCA), afirma buscar estabelecer um quadro regulamentar abrangente que ofereça proteção aos investidores enquanto promove a inovação no setor (COMMISSION, 2020).

Adoção Institucional - A adoção de criptoativos por instituições financeiras e empresas de grande porte tem crescido substancialmente. Empresas como *Tesla* e *MicroStrategy* têm incorporado Bitcoin em suas estratégias de reserva de tesouraria, sinalizando uma crescente aceitação dos criptoativos como reserva de valor (BOURI et al., 2017). Além disso, grandes instituições financeiras estão desenvolvendo produtos de investimento baseados em criptoativos, como fundos negociados em bolsa (ETFs) e contratos futuros.

Adoção pelo Consumidor - A adoção de criptoativos por consumidores está aumentando, impulsionada pela facilidade de acesso através de carteiras digitais e plataformas de negociação (KONDOR; PóSFAI; VATTAY, 2014). Serviços de pagamento como *PayPal* e *Square* permitem a compra, venda e uso de criptomoedas, tornando-as mais acessíveis ao público. Esta crescente adoção está ligada à busca por alternativas ao sistema financeiro tradicional e à percepção de criptoativos como uma forma de investimento ou proteção contra a inflação.

Inovação e Capitalização

Como apontam Nakamoto e outros pioneiros, os criptoativos, como Bitcoin e Ethereum, introduzem uma forma de moeda digital descentralizada, que “elimina a necessidade de intermediários tradicionais” (NAKAMOTO, 2008), oferecendo novas alternativas para armazenamento e troca de valor. Esse caráter descentralizado dos criptoativos impulsionou o desenvolvimento de sistemas financeiros alternativos, como a DeFi (finanças descentralizadas), que visa replicar e expandir os serviços financeiros tradicionais, oferecendo maior acessibilidade e transparência em escala global (SCHäR, 2021). O movimento de descentralização das funções cotidianas acarretam em serviços orientados à propriedade do usuário, onde dados e identidades estão sob o controle dos próprios usuários e são armazenados de maneira segura em blockchain. Exemplos dessa movimentação são os tokens-não-fungíveis e a *Web 3.0*.

Finanças Descentralizadas (DeFi) - O movimento de Finanças Descentralizadas *DeFi* representa uma das áreas mais inovadoras dentro do ecossistema de

criptoativos. Plataformas *DeFi* como *Uniswap*, *Aave* e *Compound* permitem a realização de serviços financeiros como empréstimos, trocas e investimentos de maneira descentralizada, sem a necessidade de intermediários tradicionais (ZHANG; WANG; TANG, 2020). Esses serviços são executados através de contratos inteligentes, oferecendo maior transparência e acessibilidade.

***Tokens* Não Fungíveis (NFTs)** - Os *Tokens* Não Fungíveis (NFTs) emergiram como uma nova classe de ativos digitais que representam a propriedade de itens únicos, como arte digital, música e colecionáveis. A explosão da popularidade dos NFTs em 2021 trouxe atenção significativa para o potencial de textittokenização de ativos e a criação de mercados digitais (WANG et al., 2021). Esta inovação está transformando a maneira como os direitos de propriedade e a escassez digital são percebidos e geridos.

Web 3.0 - A *Web 3.0*, também conhecida como Internet descentralizada, é uma visão que busca redefinir a estrutura da Internet, permitindo maior controle e propriedade de dados pelos usuários. Criptoativos e *Descentralized Apps* são componentes centrais desta visão, proporcionando uma infraestrutura para uma web mais segura, transparente e centrada no usuário (ZHANG; XUE; HUANG, 2019).

INCISÃO TEORICA

Ao decorrer desta pesquisa utilizamos como modelo de criptoativo o *Bitcoin*, criado pelo pseudônimo Satoshi Nakamoto. Esta moeda é, atualmente, a mais estável diante do mercado de criptoativos e a mais antiga também, percorrendo desde 2008. É manifesto neste trabalho o contexto em que o *Bitcoin* foi criado, seus objetivos diante da população e o detalhamento das tecnologias em que o ativo foi forjado.

Diante da tecnologia empregada no *Bitcoin*, neste projeto é evidenciado os pilares principais em que se apoiam o desenvolvimento das criptomoedas, definido o trilema das criptos e como este trilema impacta na execução das suas determinadas funções.

Consta também apresentado neste capítulo o conceito de *DeFi* — Sigla para Finanças Descentralizadas em inglês — e como este ecossistema tecnológico pode prover maior qualidade de vida e serviços para seus usuários.

Este projeto utiliza dos autores da Escola Austríaca de Economia — Ludwig

von Mises, Böm Bawerk, Carl Menger, Friedrich Hayek e Murray Rothbard — para induzir a definição de dinheiro e moeda, pois, com foco na definição do conceito de dinheiro é possível argumentar o quão bem uma criptomoeda cumpre este papel em comparação com a moeda de curso legal do estado.

O Bitcoin

O *Bitcoin* nasceu como um modelo de dinheiro digital que opera em uma rede descentralizada, sem a necessidade de uma autoridade central para emitir ou controlar a moeda. Foi proposto pela primeira vez em 2008 pelo programador anônimo conhecido pelo pseudônimo Satoshi Nakamoto, na documentação *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (NAKAMOTO, 2009) ,e lançado como *software* de código aberto em 2009. O *Bitcoin* permite transações *peer-to-peer* — de pessoa para pessoa e/ou ponto a ponto —, nas quais os usuários podem enviar e receber pagamentos diretamente, sem a necessidade de intermediários.

Este criptoativo é reconhecido por ser o primeiro e mais estável projeto de moeda digital e é definitivamente visto como referência de segurança, escalabilidade e descentralização no ambiente cripto. Posteriormente há uma melhor definição da tecnologia de registro em que o Bitcoin atua, a *Blockchain*.

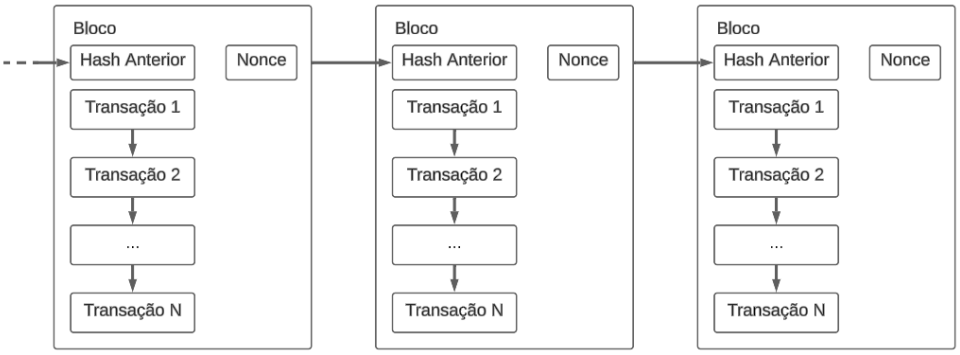
A Blockchain

A tecnologia fundamental que sustenta o *Bitcoin* é a *Blockchain*, um livro-razão digital público e distribuído que registra todas as transações de forma transparente e imutável. A *Blockchain* é composta por blocos encadeados de forma cronológica. De maneria recursiva, cada bloco contém um conjunto — por ordem temporal — de transações confirmadas de maneira encadeada e um cabeçalho que inclui um *hash* do bloco anterior, formando assim uma cadeia de blocos interligados.

Na Figura 1 exibimos uma abstração do encadeamento de blocos e seus dados diante da *Blockchain* formando a estrutura e formato da cadeia.

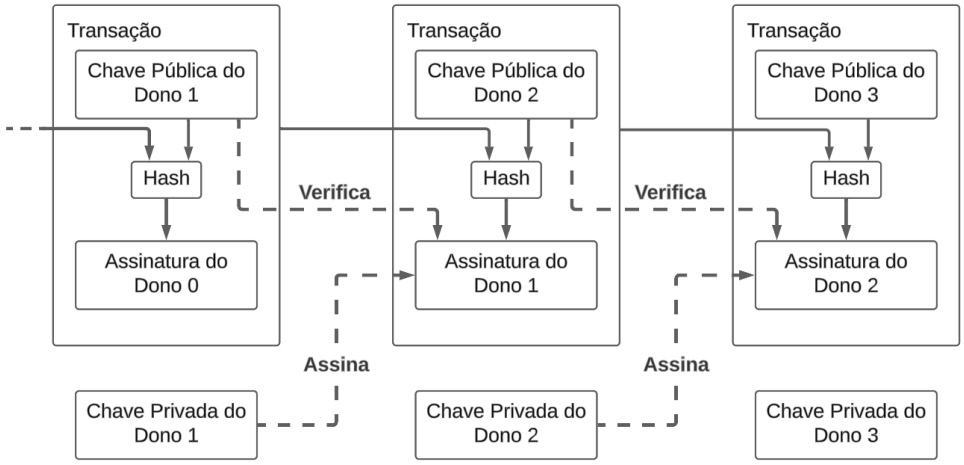
Na Figura 2 exibimos uma abstração da perspectiva do bloco, onde ocorre o encadeamento das transações seguido das suas respectivas assinaturas.

Figura 1 – Estrutura de encadeamento de blocos numa *blockchain*.



Fonte: Tradução pelos autores, baseado na documentação de referência (NAKAMOTO, 2009)

Figura 2 – Encadeamento das transações nos blocos.



Fonte: Tradução pelos autores, baseado na documentação de referência (NAKAMOTO, 2009)

Criptografia SHA-256 (Secure Hash Algorithm 256-bit)

O protocolo do Bitcoin emprega a criptografia SHA-256 (*Secure Hash Algorithm 256-bit*) como um componente fundamental para garantir a integridade e a segurança das transações na rede. Este algoritmo de *hash* criptográfico, desenvolvido pela Agência Nacional de Segurança (NSA) dos Estados Unidos e publicado pelo Instituto Nacional de Padrões e Tecnologia (NIST), é crucial para diversas operações no ecossistema Bitcoin.

O SHA-256 contribui para a segurança geral do protocolo Bitcoin por ser resistente a ataques de colisão e de pré-imagem, o que significa ser computacionalmente impraticável encontrar duas mensagens distintas que resultem no mesmo *hash* ou reverter um *hash* para obter a mensagem original. Essas propriedades são essenciais para manter a integridade das chaves e transações, garantindo que as entradas não possam ser manipuladas sem que seja facilmente detectado pela rede.

Algoritmo de Prova de Trabalho e Mineiração

Para garantir a segurança e a integridade da *Blockchain*, o *Bitcoin* utiliza um algoritmo de consenso chamado Prova de Trabalho (tambem chamado de *Proof of Work* ou PoW). Os mineradores coletam transações pendentes em um bloco e tentam gerar um *hash* válido para esse bloco usando o SHA-256.

A prova de trabalho se orienta dentro da *blockchain* diante do protocolo Merkle. O protocolo Merkle, também referido como árvore de Merkle ou *hash* de Merkle, é uma estrutura de dados fundamental em criptografia, criada por Ralph Merkle. A árvore de Merkle ajuda a garantir que os dados não foram alterados, pois, qualquer modificação nos dados de entrada alteraria o *hash* na folha correspondente e, por sua vez, todos os *hashes* no caminho até a raiz.

O algoritmo é aplicado duas vezes (conhecido como *double-SHA-256*) ao cabeçalho do bloco, que inclui a versão do programa, o *hash* do bloco anterior, o *hash* Merkle das transações no bloco, o *timestamp*, o nível de dificuldade e um *nonce*. O termo *nonce* refere-se a um número que é usado apenas uma vez (do inglês *number used once*). O *nonce* é um valor inteiro de 32 bits que os mineradores ajustam repetidamente para tentar produzir um *hash* do bloco que atenda aos critérios de dificuldade estabelecidos pela rede Bitcoin.

O objetivo é encontrar um *hash* que seja menor que o valor de dificuldade estabelecido pela rede, o que exige que os mineradores ajustem o *nonce* repetidamente e recalculam o *hash* do bloco até que um valor adequado seja encontrado. Este processo é fundamental para a implementação da prova de trabalho (*Proof of Work* - PoW), que ajuda a proteger a rede contra ataques.

Escola Austríaca de Economia

A Escola Austríaca de Economia, emergida no final do século XIX, representa uma tradição heterodoxa significativa no pensamento econômico. Caracterizada por sua ênfase na teoria subjetiva do valor, na praxeologia e no papel crucial do empreendedorismo, a Escola Austríaca oferece uma perspectiva única que contrasta com as abordagens neoclássicas e keynesianas dominantes.

Seguidamente é revisitada a história, cronologia, os principais autores e pautas centrais desta escola, destacando suas contribuições teóricas e influências dura-

douras. É constatado também definições por parte destes autores diante dos conceitos, respectivamente, de economia, capital e dinheiro

A Escola Austríaca de Economia foi fundada por Carl Menger com a publicação de *"Principles of Economics"* (1871). Seu trabalho desafiou a teoria do valor-trabalho dos economistas clássicos e introduziu a teoria marginalista do valor.

Carl Menger (1840-1921) - Em *"Principles of Economics"*, (MENGER, 1871) argumentou que o valor dos bens é determinado pela utilidade marginal que os indivíduos o atribuem, estabelecendo as bases para a análise econômica subjetiva.

Eugen von Böhm-Bawerk (1851-1914) - Discípulo de Menger, Böhm-Bawerk contribuiu significativamente para a teoria do capital e dos juros. Em *"Capital and Interest"*, ele desenvolveu a teoria da estrutura temporal da produção, enfatizando a importância do tempo no processo produtivo (BöHM-BAWERK, 1884-1889).

Friedrich von Wieser (1851-1926) - Wieser é conhecido por sua teoria do custo de oportunidade e pelo desenvolvimento da teoria do valor imputado. Ele ajudou a consolidar a Escola Austríaca como uma corrente de pensamento econômico significativa (BöHM-BAWERK, 1884-1889).

Desenvolvimento e Consolidação - No início do século XX, Ludwig von Mises e Friedrich Hayek ampliaram e consolidaram as ideias da Escola Austríaca, influenciando significativamente o pensamento econômico.

Ludwig von Mises (1881-1973) - Mises é uma figura central na Escola Austríaca. Em *"Human Action"*, ele propôs que a economia deve ser baseada na lógica dedutiva da ação humana, uma abordagem chamada praxeologia. Mises também desenvolveu a teoria do ciclo econômico, que analisa as flutuações econômicas causadas pela expansão do crédito e pela intervenção estatal no mercado monetário (MISES, 1949).

Friedrich Hayek (1899-1992) - Discípulo de Mises, Hayek contribuiu para a teoria do capital e o estudo dos ciclos econômicos. Em *"The Road to Serfdom"* e *"The Constitution of Liberty"*, Hayek criticou o intervencionismo estatal e defendeu uma ordem espontânea de mercado. Em 1974, ele recebeu o Prêmio Nobel de Economia por seu trabalho sobre a teoria monetária e as flutuações econômicas (HAYEK, 1944),(HAYEK, 1960).

Expansão e Influência Contemporânea - Na segunda metade do século XX e início do século XXI, a Escola Austríaca continuou a evoluir com novos pensadores

que expandiram suas teorias e influências.

Murray Rothbard (1926-1995) - Rothbard combinou a economia austríaca com uma filosofia libertária. Em *"Man, Economy, and State"*, ele apresentou uma visão abrangente da economia austríaca e criticou a intervenção estatal. (ROTHBARD, 1962).

Israel Kirzner (1930-) - Kirzner contribuiu para a teoria do empreendedorismo, destacando o papel do empreendedor na descoberta de oportunidades de mercado e na coordenação econômica. Seu trabalho *"Competition and Entrepreneurship"* é uma referência importante para o estudo do processo de mercado e da função empresarial (KIRZNER, 1973).

Pautas e Contribuições - A seguir consta as principais pautas da Escola Austríaca aonde servirá de base para o relacionamento dos conceitos fundamentais de economia, dinheiro e capital.

Teoria do Valor Subjetivo - A teoria do valor subjetivo é uma contribuição fundamental da Escola Austríaca. Ela afirma que o valor dos bens é determinado pela utilidade marginal atribuída pelos indivíduos, contrastando com a teoria do valor-trabalho (MENGER, 1871).

Praxeologia - A praxeologia é a metodologia central da Escola Austríaca. Baseia-se na premissa de que a economia é uma ciência social que deve ser estudada através da análise lógica da ação humana, ao invés de métodos empíricos e estatísticos (MISES, 1949).

Teoria do Ciclo Econômico - A teoria austríaca do ciclo econômico, desenvolvida por Mises e Hayek, explica as flutuações econômicas como resultado das distorções causadas pela expansão do crédito e pela intervenção governamental. Segundo esta teoria, a criação artificial de crédito leva a um mau investimento de recursos, resultando em ciclos de *boom* e *bust* (MISES, 1949; HAYEK, 1944).

Crítica ao Intervencionismo Estatal - A Escola Austríaca é fortemente crítica ao intervencionismo estatal e ao planejamento centralizado. Economistas austríacos argumentam que a intervenção governamental distorce os sinais de preço, leva a alocações ineficientes de recursos e restringe a liberdade individual. Hayek argumentou que o planejamento centralizado é incapaz de lidar com a complexidade da informação distribuída na sociedade (HAYEK, 1944; HAYEK, 1960).

Teoria do Empreendedorismo - A ênfase no papel do empreendedor é uma

característica distintiva da Escola Austríaca. Kirzner destacou que os empreendedores são essenciais para a descoberta e exploração de oportunidades de mercado, contribuindo para a coordenação econômica e a dinâmica dos mercados (KIRZNER, 1973).

Definição conceitual de maior incisão no projeto - Consta aqui definições por parte dos autores austríacos diante dos conceitos de base da atuação deste artigo. A partir desta conceitualização é possível observar diante da atuação dos criptoativos e futuramente estipular as necessidades de um sistema de moedas digitais, dedicado ao ensino de finanças.

Economia e a Ação Humana - Ludwig von Mises, em "Ação Humana"(MISES, 1949), define economia como "a ciência que estuda a ação humana, uma aplicação da teoria do conhecimento humano". Segundo Mises, a economia é um ramo da praxeologia, ou seja, a teoria da ação humana. Ele argumenta que a economia, ao contrário de ser meramente uma análise de dados e tendências, é fundamentalmente sobre como os indivíduos escolhem agir com recursos escassos para atingir seus objetivos.

Capital segundo Böhm-Bawerk - Eugen Böhm von Bawerk, contribuiu significativamente para a teoria do capital. Em sua obra *"Capital and Interest"*(BöHM-BAWERK, 1884-1889), Böhm-Bawerk descreve o capital como "bens produzidos que servem como meios para a aquisição de bens futuros"(BöHM-BAWERK, 1884-1889). Ele esclarece que o capital não é simplesmente uma acumulação de dinheiro ou ativos, mas sim ferramentas, máquinas e materiais usados para aumentar a produção futura.

Dinheiro e sua Origem para Menger - Carl Menger, foi um dos primeiros economistas a explicar a origem do dinheiro através de um processo de evolução social e não por decreto governamental ou convenção. Em sua obra "Princípios de Economia Política"(MENGER, 2017), Menger argumentou que o dinheiro emergiu organicamente como o meio mais vendável de troca, facilitando assim as transações comerciais e reduzindo os custos de transação na economia (MENGER, 1871).

Hayek e a Desestatização do Dinheiro - Friedrich Hayek, levou a teoria monetária austríaca para outra direção ao argumentar a favor da competição de moedas privadas em sua obra "Desnacionalização do Dinheiro"(HAYEK, 2017). Hayek criticou os monopólios governamentais sobre a emissão de dinheiro, propondo que a concorrência entre diferentes categorias de dinheiro poderia prevenir a inflação e promover

a estabilidade econômica.

A Teoria do Dinheiro de Mises - Ludwig von Mises expandiu a teoria de Menger ao introduzir o conceito de "regressão"em sua análise do valor do dinheiro. Em "A Teoria do Dinheiro e do Crédito"(MISES, 1914), Mises apresenta a ideia de que o valor do dinheiro hoje é derivado da expectativa de seu poder de compra no futuro, que por sua vez é baseado em uma regressão contínua até o ponto em que o dinheiro era apenas um bem mais vendável entre outros (MISES, 1914). Mises também destacou o papel do dinheiro no cálculo econômico, essencial para a alocação racional de recursos em uma economia de mercado.

Rothbard e a Crítica à Moeda Fiduciária - Murray Rothbard, seguindo a indução de Mises, foi crítico em relação ao sistema de moeda fiduciária e ao papel dos bancos centrais. Em "O que o Governo fez com o Nosso Dinheiro?"(ROTHBARD, 2022), Rothbard explica como o dinheiro historicamente ancorado em commodities, como o ouro, foi progressivamente substituído por dinheiro papel sem lastro, levando a ciclos econômicos mais instáveis e inflação.

Bitcoin é dinheiro de verdade?

Nesta secção, fazemos uma resumo do livro "*Bitcoin*, a moeda na era digital"(ULRICH, 2014) escrito por Fernando Ulrich. O brasileiro é Mestre em Economia e referência por seu pioneirismo na divulgação de criptomoedas no Brasil.

Definição de Ulrich de Dinheiro e Moeda

Em seu livro, Ulrich chega a definição de moeda como "qualquer bem econômico empregado indefinidamente como meio de troca, independentemente de sua liquidez frente a outros bens monetários e de seus possíveis usos alternativos"(ULRICH, 2014, P.89).

O autor lista atributos característicos a moeda, sendo eles sua escassez, durabilidade, homogeneidade espacial e temporal, divisibilidade e maleabilidade, comparando o desempenho destes atributos diante do papel-moeda, o ouro e o Bitcoin, como mostra na Tabela 1.

Tabela 1 – Comparação dos atributos do dinheiro diante do ouro, do papel-moeda e do *Bitcoin*

Atributos	Ouro	Papel-moeda	Bitcoin
1.Durabilidade	Alta	Baixa	Perfeita
2.Divisibilidade	Média	Alta	Perfeita
3.Maleabilidade	Alta	Alta	Incorpóreo
4.Homogeneidade	Média	Alta	Perfeita
5.Oferta(Escassez)	Limitada pela natureza	Limitada e controlada politicamente	Limitada Matematicamente
6.Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

.

Ulrich menciona também as funções do dinheiro, listadas de servir como meio de troca, reserva de valor e unidade de conta. Em outras palavras, uma moeda deve servir, respectivamente, de maneira que as suas trocas sejam de forma facilitada; deve atuar de maneira em que possa ser entesourada e/ou guardada como reserva de riqueza; e por fim permita ser utilizável como meio de conta, utilizável ao cálculo econômico em função da moeda.

Segundo Fernando, o *Bitcoin* mostra-se capaz de performar as características e as funções da moeda tão bem, se não melhor, que o ouro e o papel-moeda. De acordo com ele "apesar da aparência unicamente digital, as atuais formas de dinheiro assemelham-se em muito ao *Bitcoin*. A maior parte da massa monetária no mundo moderno manifesta-se de forma intangível; nosso dinheiro já é um bem incorpóreo, uma característica que em nada nos impede de usá-lo diariamente"(ULRICH, 2014, p.95).

ESTUDO DA ARQUITETURA *BLOCKCHAIN* UTILIZANDO RUST

Utilizamos de uma implementação experimental e educativa, que explica os princípios fundamentais da tecnologia *blockchain* e explora os recursos da linguagem Rust que a tornam adequada para esse tipo de aplicação. Rust é amplamente reconhecida por seu gerenciamento de memória seguro e por evitar vulnerabilidades comuns a linguagens como C++ (MATSAKIS; KLOCK, 2014), o que é crucial no desenvolvimento de sistemas descentralizados e imutáveis, como uma *blockchain*.

Introdutoriamente utilizamos como base as seguintes fontes de conteúdo:

- **Documentação do *Bitcoin*** (NAKAMOTO, 2008): Esta documentação foi utili-

zada por conta da orientação do projeto sob a arquitetura do *Bitcoin*.

- **Documentação do *Rust - Programming Language*** (Rust Project Developers, 2024): Esta documentação foi utilizada pela tratativa da utilização do Rust como linguagem principal do projeto.
- **Documentação do pacote Rust de requisições - Actix Web** (Actix Web Contributors, 2024): Esta documentação foi utilizada por conta da possivel exibição da *blockchain* sob hospedagem e tratativa de requisições.
- **Coleção de video-aulas *"Blockchain in Rust"*** (Jacob Lindahl (GeekLaunch), 2019): Esta coleção de aulas foram selecionadas como referência devida a sua contextualização orientada tanto ao *Bitcoin* quanto ao Rust com a ressalva da ótima capacidade didática do autor.

Estutura Geral do Código

Sob Perspectiva panorâmica, nosso projeto em Rust conta com as seguintes estruturas: ***Outputs*, Transações, Blocos e a *Blockchain***. Estas estruturas são as classes por onde a organização da nossa corrente registra seus dados, sob elas adicionamos *outputs* às transações, adicionamos transações aos blocos, adicionamos blocos às correntes e aderessamos cada objeto aos seus devidos *hashes*.

Estrutura da Transação

Em nosso estudo de arquitetura, as transações são compostas por **entradas** (*inputs*) e **saídas** (*outputs*), referenciando o valor, quem será debitado e quem será creditado após a transação. Salve a consideração que transações sem entrada definida, que são chamadas de "transações de base monetária". Diferentemente do *Bitcoin*, em nosso projeto transações desta natureza são permitidas a fim de exemplificar o comportamento inflacionário sob o aumento da base monetária.

Seguindo a nossa referência, na documentação do *Bitcoin*, vemos que as entradas nas transações na verdade são representações das saídas de transações anteriores, estabelecendo que apenas possamos gastar moedas que previamente nos foram dadas.

Estutura do Bloco

Conforme verificamos anteriormente, uma *blockchain* é uma estrutura de dados distribuída e imutável composta por blocos interligados que contêm registros de transações (NAKAMOTO, 2008). No desenvolvimento dessa estrutura em Rust, cada bloco da *blockchain* contém os seguintes elementos:

- **Índice:** Define a posição do bloco na cadeia.
- ***Timestamp*:** Marca o horário de criação do bloco.
- **Lista de transações:** Conjunto de dados que representa as operações contidas no bloco.
- **Hash do bloco anterior:** Garantia de encadeamento entre os blocos.
- **Hash do bloco atual:** Gerado a partir dos dados do bloco para garantir sua integridade e imutabilidade.
- **Dificuldade:** Representa o nível de dificuldade atual do bloco durante sua mineração.
- ***Nonce*:** Número gerado durante o processo de prova-de-trabalho.

Essa arquitetura de blocos tem como orientação o padrão proposto por Satoshi e é implementada em Rust por meio de dados estruturados. Rust permite encapsular esses dados de forma eficiente, maximizando a segurança e minimizando o risco de falhas de memória (MATSAKIS; KLOCK, 2014).

Implementação da Estrutura da Blockchain

A estrutura da blockchain propriamente dita é composta por uma lista de blocos e métodos para adicionar novos blocos, além de validar a cadeia. Em nossa implementação, seguimos o padrão de encadeamento proposto por Nakamoto, mantendo o último bloco adicionado como referência para o próximo.

Seguimos também com as verificações que ocorrem na corrente durante a adição de novos blocos, nem todas verificações foram possíveis de implementar devido à limitante do caráter educativo do estudo. Portanto foram implementadas as seguintes verificações, diante de seus respectivos códigos de erro:

- `MismatchedIndex`: Verificação do posicionamento de blocos na corrente;
- `InvalidHash`: Verificação dos *Hahes* de cada bloco diante de sua dificuldade;
- `AchronologicalTimestamp`: Verificação da marca temporal dos blocos;
- `MismatchedPreviousHash`: Verificação do apontamento de *Hahes* dos blocos;
- `InvalidGenesisBlockFormat`: Verificação da formatação do bloco primeiro bloco (gênesis da corrente);
- `InvalidInput`: Verificação do apontamento de entrada das transações;
- `InsufficientInputValue`: Verificação da quantidade de moedas apontadas durante a entrada das transações;

Implementação da Hospedagem

Durante nosso estudo, implementamos o *backend* da nossa aplicação de *blockchain* utilizando a biblioteca Rust Axtix Web. Neste sistema implementamos apenas a criação programática da corrente, a exibição geral de dados dos blocos, a exibição detalhada de cada bloco, e a introdução de novos blocos via requisições JSON.

A seguir é apresentado imagens desta experimentação, o repositório [2] onde o código e os arquivos deste teste foram armazenados na plataforma Github por preferência dos autores.

Na Figura 3 consta o registro via terminal Linux das atualizações realizadas na *Blockchain*:

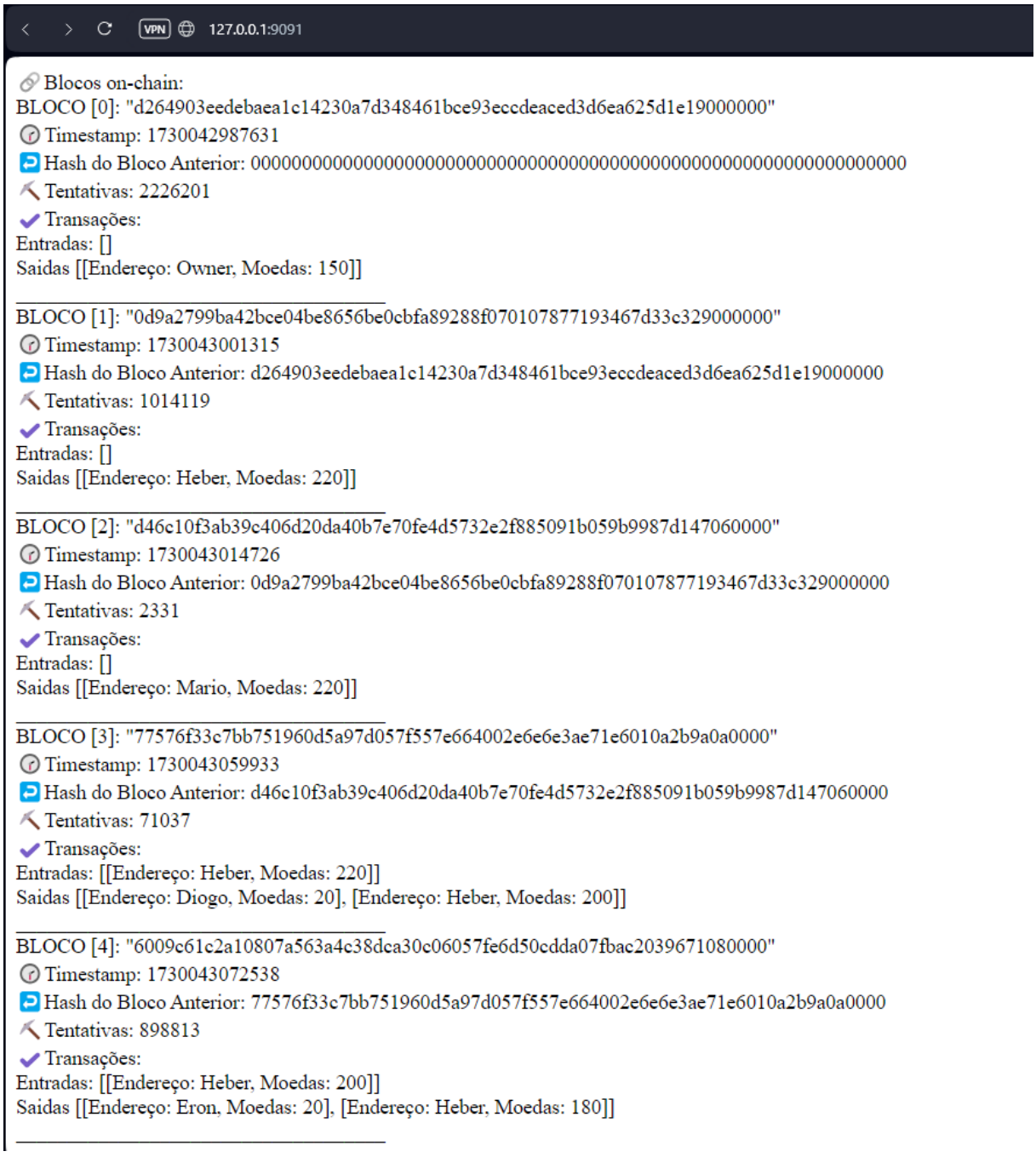
Figura 3 – Resposta via terminal sobre as atualizações na *Blockchain*.

Fonte: Captura de tela tirada pelos autores

[2] https://github.com/HeberUnifil/Educational-Blockchain-Currency

Na Figura 4 consta a exibição geral dos blocos ordenados na corrente, seus respectivos *hashes*, sua marca temporal, quantidade de transações e o número de tentativas para mineração do bloco.

Figura 4 – Resposta via terminal sobre as atualizações na *Blockchain*.



Fonte: Captura de tela tirada pelos autores

CONCLUSÃO

Neste projeto, percorremos por meio do contexto técnico e social do desenvolvimento dos criptoativos, averiguamos a motivação de desintermediação das atividades financeiras por meio da origem do *Bitcoin*; exploramos o ecossistema cripto por meio dos contratos inteligentes e da *DeFi*, e exibimos seu impacto diante da economia tradicional.

Apresentamos os conceitos chave do funcionamento do *Bitcoin*, constatamos a estrutura dos blocos, a estrutura do encadeamento, o procedimento de prova de trabalho utilizado na mineração do *Bitcoin* e como constitui o seu caráter criptográfico. Vimos também como a natureza do *Bitcoin*, de maneira programática, corrobora aos conceitos técnico-economicos da Escola Austríaca de Economia, provendo respaldo diante das características do dinheiro, tão bem como as funções da moeda. Apresentamos o resultado da comparação de suas características ao papel-moeda e ao ouros por Fernando Ulrich.

Por fim, atuamos na experimentação educacional da implementação de um sistema de *blockchain* de nível médio, que abstrai os conceitos base do *Bitcoin*, permite a manipulação via requisições e exibe as classes presentes da corrente no navegador. Foi exposto todas as estruturas geradas neste experimento, seus atributos e suas funções diantes da rede.

Escrever um paragrafo como esse trabalho poderia ser melhorado, ou como ele poderia ser continuado. Quais pontos você acha que poderiam ser mais explorados?

REFERÊNCIAS

Actix Web Contributors. *Actix Web Documentation*. 2024. Accessed: 2024-10-26. Disponível em: <https://actix.rs/docs/>. 16

AUER, R.; CLAESSENS, S. Regulating cryptocurrencies: Assessing market reactions. *BIS Quarterly Review*, 2018. 5

BOURI, E. et al. On the hedge and safe haven properties of bitcoin: Is it really more than a diversifier? *Finance Research Letters*, Elsevier, v. 20, p. 192–198, 2017. 6

BUTERIN, V. *Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform*. 2013. <https://github.com/ethereum/wiki/wiki/White-Paper>. 5

BöHM-BAWERK, E. v. *Capital and Interest*. [S.l.]: Macmillan, 1884–1889. 11, 13

COMMISSION, E. *Proposal for a Regulation on Markets in Crypto-assets*. 2020. <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12447-Framework-for-markets-in-crypto-assets>. 6

FATF, F. A. T. F. *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. 2019. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html>. 5

HAYEK, F. A. *The Road to Serfdom*. [S.l.]: University of Chicago Press, 1944. 11, 12

HAYEK, F. A. *The Constitution of Liberty*. [S.l.]: University of Chicago Press, 1960. 11, 12

HAYEK, F. A. *Desestatização do dinheiro*. [S.l.]: LVM Editora, 2017. 13

Jacob Lindahl (GeekLaunch). *Blockchain in Rust*. 2019. YouTube. Accessed: 2024-10-26. Disponível em: <https://www.youtube.com/playlist?list=PLwnSaD6BDfXL0RiKT_5nOIdxTxZWpPtAv>. 16

KIRZNER, I. M. *Competition and Entrepreneurship*. [S.l.]: University of Chicago Press, 1973. 12, 13

KONDOR, D.; PóSFAI, M.; VATTAY, G. Do the rich get richer? an empirical analysis of the bitcoin transaction network. *PLOS ONE*, Public Library of Science, v. 9, n. 2, p. e86197, 2014. 6

KWON, J. *Cosmos: A Network of Distributed Ledgers*. 2016. <https://cosmos.network/resources/whitepaper>. 5

MATSAKIS, N.; KLOCK, F. The rust language. In: *Proceedings of the ACM SIGAda Annual Conference on High Integrity Language Technology*. [S.l.: s.n.], 2014. p. 103–104. 15, 17

MENGER, C. *Principles of Economics*. [S.l.]: Braumüller, 1871. 11, 12, 13

MENGER, C. *LIBERALISMO-Carl Menger: Princípios de Economia Polí tica*. [S.l.]: LeBooks Editora, 2017. 13

MISES, L. V. *The theory of money and credit*. [S.l.]: Oxford University Press, 1914. 14

MISES, L. v. *Human Action: A Treatise on Economics*. [S.l.]: Yale University Press, 1949. 11, 12, 13

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. <https://bitcoin.org/bitcoin.pdf>. 6, 15, 17

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. maio 2009. Disponível em: <http://www.bitcoin.org/bitcoin.pdf>. 4, 8, 9

ROTHBARD, M. N. *Man, Economy, and State: A Treatise on Economic Principles*. [S.l.]: D. Van Nostrand Company, 1962. 12

ROTHBARD, M. N. *O que o Governo Fez com o Nosso Dinheiro?* [S.l.]: LVM Editora, 2022. 14

Rust Project Developers. *Learn Rust Programming Language*. 2024. Accessed: 2024-10-26. Disponível em: <https://www.rust-lang.org/learn>. 16

SCHäR, F. Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, v. 103, n. 2, p. 153–174, 2021. 6

ULRICH, F. Bitcoin-a moeda na era digital. *Mises Brasil*, v. 2, p. 239, 2014. Disponível em: <https://hmd.adm.br/ebooks/diversos/Bitcoin-AMoedaDigital.pdf>. 14, 15

WANG, Q. et al. Non-fungible token (nft): Overview, evaluation, opportunities and challenges. *arXiv preprint arXiv:2105.07447*, 2021. 7

WOOD, G. *Polkadot: Vision for a Heterogeneous Multi-chain Framework*. 2016. <https://polkadot.network/PolkaDotPaper.pdf>. 5

YETMAR, S. A. What is cryptocurrency? *Journal of Business Theory and Practice*, 2023. Disponível em: <https://api.semanticscholar.org/CorpusID:240345041>. 1

ZHANG, P.; XUE, X.; HUANG, X. A secure system for pervasive social network-based healthcare. *IEEE Access*, IEEE, v. 7, p. 116075–116088, 2019. 7

ZHANG, R.; WANG, Y.; TANG, J. Data privacy for blockchain and ai convergence: Challenges and opportunities. *IEEE Access*, IEEE, v. 8, p. 21091–21101, 2020. 7

ZOHAR, A. Bitcoin: under the hood. *Communications of the ACM*, ACM New York, NY, USA, v. 58, n. 9, p. 104–113, 2015. 5