CIENCIAS DA COMPUTAÇÃO

HEBER JOSÉ DA SILVA JUNIOR

UM ESTUDO TÉCNICO DAS CRIPTOMOEDAS E O CONCEITO DE UM CRIPTOATIVO NO ENSINO DE FINANÇAS

Londrina

2024

HEBER JOSÉ DA SILVA JUNIOR

UM ESTUDO TÉCNICO DAS CRIPTOMOEDAS E O CONCEITO DE UM CRIPTOATIVO NO ENSINO DE FINANÇAS

Trabalho de Dissertação apresentado ao Centro Universitário Filadélfia como parte dos requisitos para obtenção de graduação em Ciencias da Computação. Orientador: Mario Henrique Akihiko da Costa Adaniya.

Londrina
2024

JUNIOR; HEBER. **Um Estudo Técnico das Criptomoedas e o Conceito de um Criptoativo no Ensino de Finanças**. Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Filadélfia. Londrina, 2024.

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-chaves: Tecnologia financeira; Economia; Blockchain; Bitcoin; Educação financeira; Criptoativos; DeFi.

SUMÁRIO

1 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. 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 distribuído. 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 secção 5.1 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 secção 5.2 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 secção 5.3 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.

Futuramente, na secção 5.4, 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.

2 PROBLEMÁTICA DA PESQUISA

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, 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 de "Minhas chaves, minhas moedas".

3 METODOLOGIA DE PESQUISA

4 RESULTADOS ESPERADOS

Tendo posto o entendimento do funcionamento dos criptoativos, seus objetivos, suas problemáticas e seu devido posicionamento como dinheiro, este trabalho visa clarificar a população geral a possibilidade da adoção do ambiente DeFi e apresentar uma centelha de liberdade e autonomia financeira ao leitor enquanto olha para fora do ambiente tradicional de mercado.

Este projeto almeja também a possibilidade de simular e/ou conteinerizar os movimentos da economia dentro de um protocolo DeFi, que seria posteriormente dedicado a usar tal simulação para o ensino de finanças.

O funcionamento deste protocolo deverá seguir as movimentações econômicas baseadas nos autores austríacos mencionados previamente enquanto preserva as qualidades de segurança do *Bitcoin* e provê autonomia para professores manipularem o ambiente simulado e experienciar movimentações de resposta teorizadas diante da economia.

4.1 LIMITAÇÕES DO TRABALHO

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.

5 ESTADO DA ARTE

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 apresentado também o conceito de DeFi — Também entendido como finanças descentralizadas — 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.

5.1 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 não identificado conhecido como Satoshi Nakamoto (na documentação "Bitcoin: A Peer-to-Peer Electronic Cash System") 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.

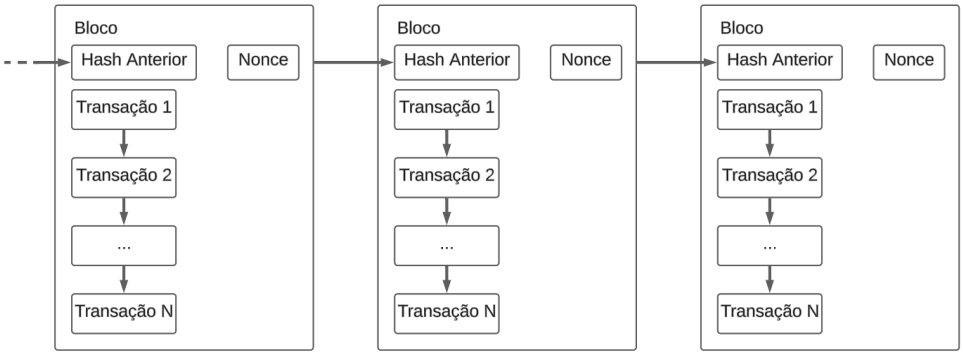
Na subsecção 5.1.1 é explicada a tecnologia de registro em que o Bitcoin atua, a Blockchain.

5.1.1 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 é possível visualizar o formato em que a estrutura de Blockchain é formada.

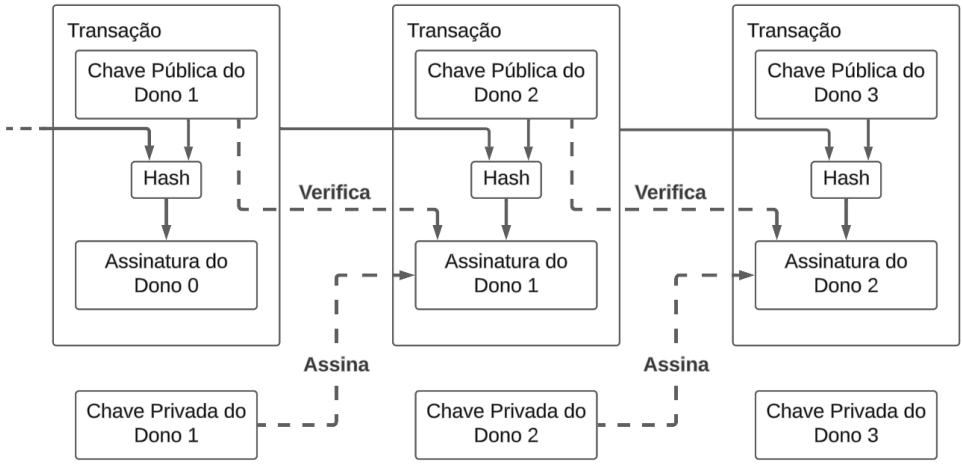
Figura 1 – Estrutura de encadeamento de blocos numa blockchain.



Fonte: os autores

Na Figura 2 é possível visualizar a estrutura de encadeamento das transações nos blocos.

Figura 2 – Encadeamento das transações nos blocos. Fonte: Os autores



Fonte: os autores

Na subsecção 5.1.2 é explicada a tecnologia de criptografia utilizada na atuação do Bitcoin.

5.1.2 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 dentro do 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 que é 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 isso seja facilmente detectado pela rede.

5.1.3 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.

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[1] das transações no bloco, o *timestamp*, o nível de dificuldade e um *nonce*[2].

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.

---

[1] 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.

[2] 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.

5.2 ESCOLA AUSTRÍACA DE ECONOMIA

O estudo da economia envolve a análise profunda de conceitos como economia, capital, dinheiro e crédito. Os economistas da Escola Austríaca, incluindo figuras proeminentes como Ludwig von Mises, Eugen Böhm von Bawerk, Carl Menger, Friedrich Hayek e Murray Rothbard, têm oferecido interpretações e teorias influentes que se diferenciam significativamente das abordagens mais tradicionais.

5.2.1 Economia e a Ação Humana

Ludwig von Mises, em sua obra "Ação Humana", define economia como "a ciência que estuda a ação humana, uma aplicação da teoria do conhecimento humano"(Mises, 1949). 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.

5.2.2 Capital segundo Böhm-Bawerk

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

5.2.3 Dinheiro e sua Origem para Menger

Carl Menger, considerado o fundador da Escola Austríaca, 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"(1871), 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).

5.2.4 Hayek e a Desnacionalização do Dinheiro

Friedrich Hayek, ganhador do Prêmio Nobel, levou a teoria monetária austríaca para outra direção ao argumentar a favor da competição de moedas privadas em sua obra "Desnacionalização do Dinheiro"(1976). Hayek criticou os monopólios governamentais sobre a emissão de dinheiro, propondo que a concorrência entre dife-

rentes tipos de dinheiro poderia prevenir a inflação e promover a estabilidade econômica (Hayek, 1976).

5.2.5 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"(1912), 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, 1912). Mises também destacou o papel do dinheiro no cálculo econômico, essencial para a alocação racional de recursos em uma economia de mercado.

5.2.6 Rothbard e a Crítica à Moeda Fiduciária

Murray Rothbard, seguindo a tradição 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?"(1963), 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 (Rothbard, 1963).

5.3 BITCOIN É DINHEIRO DE VERDADE?

Nesta secção, fazemos uma revisão do livro "Bitcoin, a moeda na era digital"(1ª Edição; Instituto Mises Brasil; 2014) escrito por Fernando Ulrich. O brasileiro é Mestre em Economia e referência por seu pioneirismo na divulgação de criptomoedas no Brasil.

Definição Unificada 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"[3].

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 Figura 3.

[3] Página.89

Figura 3 – Estrutura de encadeamento de blocos numa blockchain.

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	Ilimitada e controlada politicamente	Limitada matematica-mente
6. Dependência de terceiros fiduciários	Alta	Alta	Baixa ou quase nula

Fonte: Bitcoin, a moeda na era digital; Ulrich,Fernando; 2014; p.67.

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"[4].

5.4 UM CRIPTOATIVO EDUCATIVO

[4] Página 95

REFERÊNCIAS