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

Criptomoedas têm conquistado seu caminho no cenário financeiro global, trazendo uma nova perspectiva 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 o aprendizado tanto das ciências econômicas, quanto de algoritmos criptográficos, segurança e infraestrutura de dados. Este artigo apresenta as bases das moedas digitais, suas tecnologias empregadas e seu impacto sobre a economia tradicional. Além disso é explorada a técnica diante da estrutura do *Bitcoin*, os conceitos de dinheiro sob a visão dos autores presentes na Escola Austríaca de Economia e como a tecnologia aplicada deste criptoativo programaticamente se orienta aos conceitos austríacos de dinheiro. É apresentado por fim um estudo prático, de viés exploratório e educacional, da arquitetura de *Blockchain* do *Bitcoin* utilizando a linguagem de programação Rust.

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

Abstract

Cryptocurrencies have made their way onto the global financial scene, bringing a new perspective to economic transactions. The rise of digital currencies such as Bitcoin and Ethereum has brought with it not only a revolution in financial technology, but also a wave of speculation, debate and innovation. However, in addition to its potential as an investment vehicle and medium of exchange, the world of cryptoassets also opens doors for learning about economic sciences, cryptographic algorithms, security and data infrastructure. This article presents the basics of digital currencies, their technologies and their impact on the traditional economy. Also is explored the technical structure of Bitcoin, the concepts of money from the point of view of the authors of the Austrian School of Economics and how the applied technology of this crypto-asset is programmatically oriented towards Austrian concepts of money. Finally, a practical, exploratory and educational study of the Blockchain architecture of Bitcoin using the Rust programming language is presented.

Keywords: Financial technology; Economics; Austrian Economics; Blockchain; Bitcoin; Financial education; Cryptoassets; DeFi; Rust. english

INTRODUÇÃO

Embora as criptomoedas tenham ganhado destaque recentemente, a compreensão abrangente de seu estado técnico atual permanece fragmentada, a falta de clareza popular diante do contexto de criptoativos torna o conceito menos palatável à aceitação pública da tecnologia. Embora compreensível a baixa adesão popular a tal

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

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*).

De acordo com o mestre em desenvolvimento econômico Pedro Lopes Marinho, em 2001, devido ao início da Primeira Guerra Mundial, o sistema monetário padrão-ouro foi mundialmente abolido enquanto governos financiavam gastos militares a partir da emissão de novas 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 estão sob alto risco de serem descartadas por mal uso governamental 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”. 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 em geral operam em redes descentralizadas, 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.

Neste projeto, foi utilizado o *Bitcoin* como exemplo, de modo a verificar o con-

texto da criação e aplicação deste ativo, seu posicionamento sobre o dinheiro tradicional e como é possível utilizar do ambiente das criptos sob a perspectiva de independência monetária. Além disso é apresentada a tecnologia de encadeamento e rede em que o *Bitcoin* atua, a *Blockchain*, detalhando o funcionamento da moeda na assinatura de transações por meio da criptografia de chave pública e privada e a validação de novos blocos por meio da tecnologia Prova de Trabalho, ou *Proof of Work*.

São adotadas neste trabalho as definições de dinheiro e moeda da Escola Austríaca de Economia. Detalhamos brevemente os conceitos da ciência financeira, evidenciando a abordagem e abstração tecnológica do criptoativo diante da teoria.

Por fim, neste projeto, realizamos um estudo da arquitetura apresentada de *Blockchain* do *Bitcoin* utilizando a linguagem de programação Rust. Com viés exploratório e educacional tanto da arquitetura quanto da linguagem de programação, Foi apresentado os resultados desta experimentação.

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-chave: Criptoativos, *Bitcoin*, *Smart Contracts*, *Blockchain*, *DeFi* e *Web 3*. Foi utilizada a revisão destes artigos de modo a buscar o estado da arte documentada 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 retornou um total de 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 realizada uma busca complementar pelas referências bibliográficas da Escola Austríaca de Economia — devido à semelhança do comportamento agnóstico às instituições governamentais tanto desta vertente acadêmica quanto das finanças descentralizadas — no que foi considerada busca de literatura de seus principais

autores. Esta segunda filtragem retornou um total de 7 livros e 27 artigos.

A partir da leitura de toda a documentação coletada, foi obtido o estado da arte e contexto social diante da utilização de criptoativos, tais como serviços, propostas e ferramentas. Foi registrada também a atuação técnica da moeda digital mais utilizada atualmente, o *Bitcoin* (Conforme o indexador de criptoativos *CoinGecko*, acessado 22/05/2024), registrado o comportamento do ativo na perspectiva da Escola Austríaca de Economia, verificada a comparação do ativo digital diante do ouro e o papel-moeda e validado como a tecnologia do *Bitcoin* programaticamente se apoia a leitura teórica de economia.

Por fim, foi realizado um estudo exploratório e prático da arquitetura de *Blockchain* do *Bitcoin*, nesta etapa foram analisadas linguagens de baixo nível, ou seja, mais próximas da linguagem de máquina a fim de reduzir o gasto computacional durante o desenvolvimento e testes; foi escolhida a linguagem de programação *Rust* e pesquisada diante da sua documentação em conjunto com sua possível aplicação em arquiteturas de encadeamento de blocos; toda a programação foi versionada na plataforma *Github* e expostas diante desta documentação, abrindo as oportunidades para melhoria e aprimoramento do código em trabalhos futuros.

ESTADO DA ARTE E CAPITALIZAÇÃO

Nakamoto e outros pioneiros destacam que 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 um ecossistema financeiros alternativos, oferecendo maior acessibilidade e transparência em escala global (SCHäR, 2021). O movimento de descentralização das funções cotidianas acarretam na capitalização de serviços orientados a propriedade do usuário, onde dados e identidades estão sob o controle dos próprios usuários e são armazenados de maneira segura em blockchain. Neste sentido, novas tecnologias foram adotadas diante da implementação das criptomoedas e, tais inovações constam detalhadas nas seções a seguir.

Blockchain e Tecnologia de Registro Distribuído (DLT)

A *blockchain*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). Na fundamentação teórica consta detalhadamente o processo de encadeamento, mineração e adição de novos blocos numa blockchain.

Contratos Inteligentes

Contratos inteligentes *(smart contracts)* são programas auto executáveis 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*. A 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.

ACEITAÇÃO 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, cri-

ando 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.

FUNDAMENTAÇÃO TEÓRICA

Ao decorrer desta pesquisa foi utilizado como modelo de criptoativo o *Bitcoin*. Diante da tecnologia empregada no *Bitcoin*, a seguir consta evidenciada a funcionali-

dade, a motivação para que o sistema foi desenvolvido e o detalhamento técnico das suas partes.

Este projeto utilizou dos autores da Escola Austríaca de Economia Böm Bawerk, Carl Menger e Friedrich Hayek, Ludwig von Mises, junto com a incisão do economista Fernando Ulrich para buscar uma definição de dinheiro e moeda. Por fim é verificado o quão bem a tecnologia embarcada do *Bitcoin* cumpre seu papel de moeda em comparação com o ouro e com o papel-moeda.

Detalhamento Técnico do *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 usuários podem enviar e receber pagamentos diretamente, sem a necessidade de intermediários.

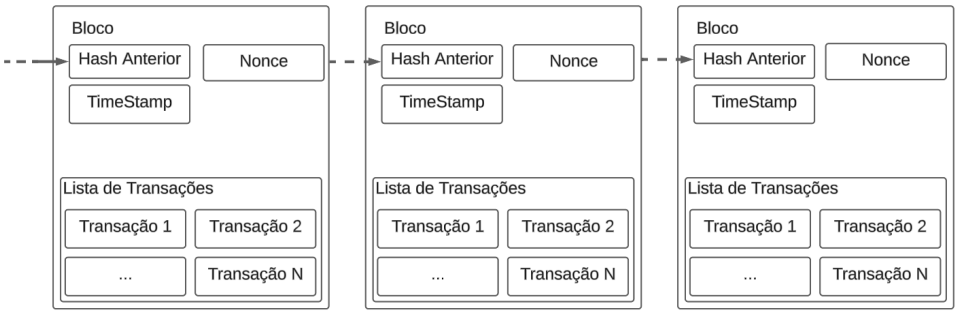
Este criptoativo é reconhecido por ser o primeiro e mais estável projeto de moeda digital e é definitivamente visto como referência de segurança, escalabilidade e descentralização no ambiente cripto. Posteriormente há uma melhor definição da tecnologia de registro em que o Bitcoin atua.

A Blockchain - A 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, ao passo que toda adição à corrente é seguida da replicação e constante validação dos usuários da rede.

O Bloco - De maneira simplificada, estrutura do bloco contém primeiramente os dados de *header* do bloco, dados que são utilizados para a geração do *hash* do bloco, como o *hash* do bloco anterior, a marca de tempo da criação do bloco e o número de tentativas de mineração. Em seguida, o bloco armazena as transações já confirmadas numa lista cronológica. Na Figura 1 é exibido uma representação gráfica do encadeamento de blocos e seus dados diante da *Blockchain* formando a estrutura

e formato da cadeia.

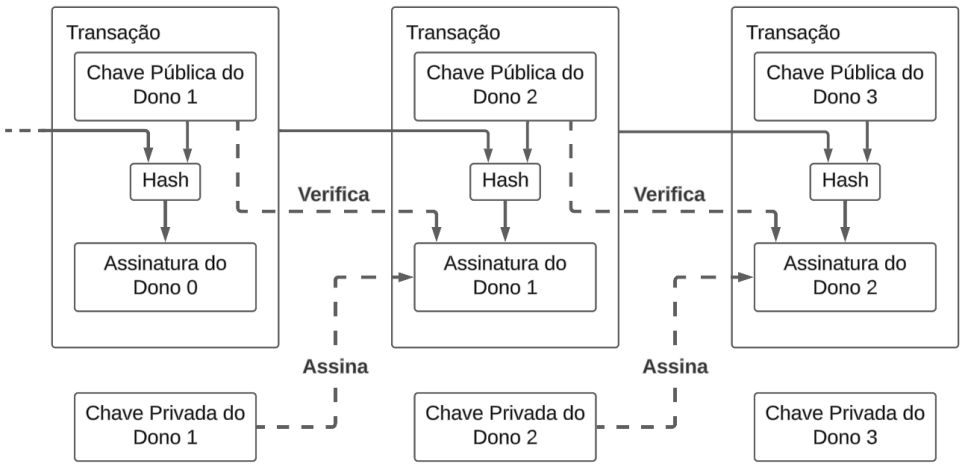
Figura 1 – Estrutura de encadeamento de blocos numa *blockchain*.



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

As Transações - A classe de transação do *Bitcoin* armazena da chave criptográfica pública do dono atual das moedas e da assinatura criptográfica do dono anterior, no intuito de impedir que um usuário gaste moedas que não recebeu, dando lastro às trocas. Durante a adição das transações aos blocos, é verificado recursivamente se o lastro de cada troca não foi utilizado previamente, evitando que um usuário gaste mais de uma vez as moedas que recebeu. Na Figura 2 é exibido uma abstração das transações, onde a transação anterior valida a realização da subsequente, assim dando histórico a cada transação efetuada entre os blocos.

Figura 2 – Encadeamento dos lastro das transações entre os blocos.

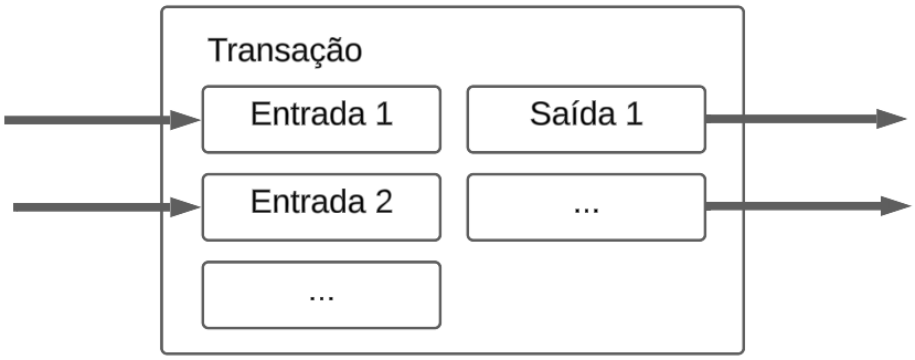


Fonte: Tradução pelos autores, baseado na documentação de referência (NAKAMOTO, 2009)

Para evitar a necessidade de realizar uma transação separada para cada fração de valor, as transações permitem que o montante seja dividido e combinado conforme necessário. Assim, as transações podem conter várias entradas e saídas. Em geral, há uma única entrada, originada de uma transação anterior de valor maior, ou

várias entradas que somam valores menores. Quanto às saídas, geralmente há duas: uma para o destinatário do pagamento e, se houver excedente, outra para devolver o troco ao remetente. É importante salientar que a representação de entrada, performativamente é sempre o objeto de saída da transação de lastro anterior, como explicado no parágrafo anterior. Na Figura 3 é exibido uma representação gráfica do processo de entradas e saídas das transações.

Figura 3 – Processo de entradas e saídas nas transações.



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

Criptografia utilizada, 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. O SHA-256 contribui para a segurança geral do protocolo 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 Mineração - O *Bitcoin* utiliza um algoritmo de consenso chamado Prova de Trabalho (também chamado, do inglês, 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, de maneira mais detalhada, 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.

A TECNOLOGIA DO *BITCOIN* COMO DINHEIRO

A partir da literatura da Escola Austríaca de Economia e do resumo apresentado no livro “*Bitcoin*, a moeda na era digital” escrito por Fernando Ulrich, é possível induzir 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).

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).

A partir do livro *"Capital and Interest"*(BöHM-BAWERK, 1884-1889), Bawerk descreve o capital como "bens produzidos que servem como meios para a aquisição de bens futuros". esclarecendo que o capital não é simplesmente uma acumulação de dinheiro ou ativos, mas sim ferramentas, máquinas e materiais usados para aumentar a produção futura.

De modo mais incisivo, Ulrich lista atributos característicos a moeda e a dependência de terceiros fiduciários, como mostra na Tabela 1, e compara a capacidade

performática do ouro, do papel-moeda e do *Bitcoin*. Sendo os atributos do dinheiro:

- **Durabilidade:** Capacidade de resistência ao tempo;
- **Divisibilidade:** Capacidade de fracionamento;
- **Maleabilidade:** Capacidade de transferência;
- **Homogeneidade:** Capacidade de representação de valor equivalente;
- **Oferta(Escassez):** Incapacidade de ser duplicável;
- **Dependência de terceiros fiduciários:** O quão dependente o usuário é de um ator terceiro;

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

Fonte: "*Bitcoin*, a moeda na era digital"(ULRICH, 2014)

O autor 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, senão 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 DE *BLOCKCHAIN* UTILIZANDO RUST

Foi utilizada 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*. Por fim de teste, foi aplicado um comparativo da velocidade de processamento da linguagem *Rust* com a linguagem *Python3* e foi constatada uma diferença de performance do *Rust* cinco vezes maior que do *Python3*.

Foi usado como base de conhecimento as seguintes fontes de conteúdo:

- **Documentação do *Bitcoin*** (NAKAMOTO, 2008): Esta documentação foi utilizada 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 possÍvel 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 adereçamos 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 *Hashes* de cada bloco diante de sua dificuldade;
- `AchronologicalTimestamp:` Verificação da marca temporal dos blocos;
- `MismatchedPreviousHash:` Verificação do apontamento de *Hashes* 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;

Exibição da *Blockchain* via Terminal e Navegador

Durante nosso estudo, foi adotado o *backend* da aplicação de *blockchain* utilizando a biblioteca Rust Actix Web. Neste sistema foi implementado apenas apenas

duas rotas, pois o objetivo deste *backend* seria apenas inserir novos blocos à sequência e exibir detalhadamente no navegador o estado dos blocos diante da corrente, sendo as rotas:

- **Rota GET** ‘‘/’’: Esta rota é dedicada a exibição detalhada de dados dos blocos, ela coleta todos os blocos da corrente, os ordena e exibe os dados de Index, *Hash*, *Hash* do bloco anterior, quantidade de tentativas na mineração e as transações contida no bloco, com suas respectivas entradas e saídas de moedas;
- **Rota POST** ‘‘`/add`’’: Esta rota é dedicada a receber um arquivo JSON, contendo os dados de remetente, destinatário, valor de entrada e valor de saída de moedas, considerando que a ausência de remetente caracteriza-se como uma transação de base monetária.

Consta em seguida as imagens desta experimentação, o repositório [1] onde o código e os arquivos deste teste foram armazenados na plataforma Github por preferência dos autores.

Na Figura 4 consta o registro via terminal Linux do histórico das atividades realizadas na *Blockchain*:

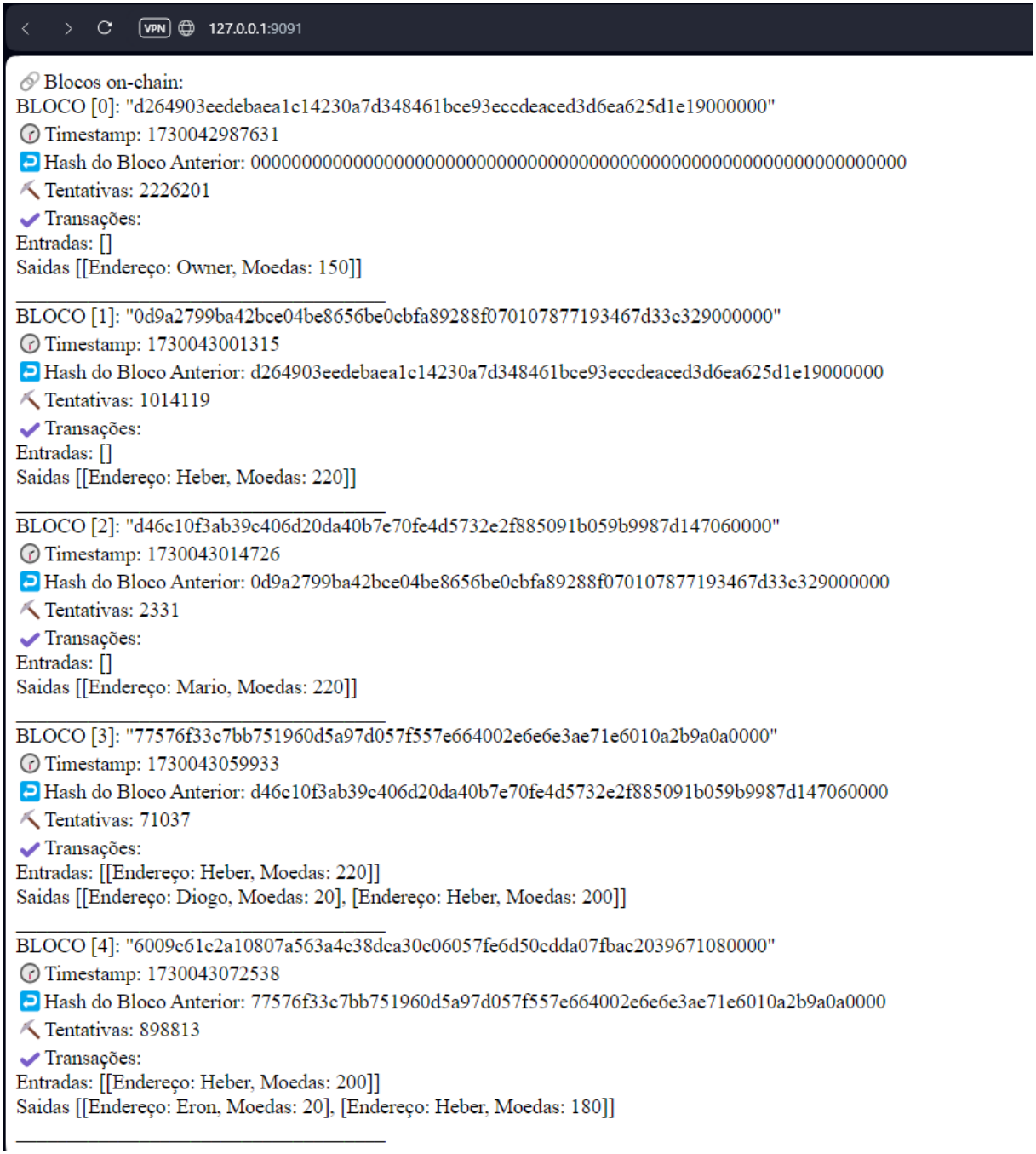
Figura 4 – Resposta via terminal sobre as atualizações na *Blockchain*.

Fonte: Captura de tela tirada pelos autores

Na Figura 5 consta no navegador a exibição detalhada dos blocos ordenados na corrente, seus respectivos *hashes*, sua marca temporal, quantidade de transações e o número de tentativas para mineração do bloco:

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

Figura 5 – Resposta via navegador sobre o estado da *Blockchain*.



Fonte: Captura de tela tirada pelos autores

CONCLUSÃO

Neste projeto, foi percorrido por meio do contexto técnico e social do desenvolvimento dos criptoativos, averiguado a motivação de desintermediação das atividades financeiras por meio da origem do *Bitcoin*; explorado o ecossistema cripto por meio dos contratos inteligentes e da *DeFi*, e é exibido seu impacto diante da economia tradicional.

Foi apresentado os conceitos chave do funcionamento do *Bitcoin*, constatado 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. Foi visto também como a natureza do *Bitcoin*, de maneira programática, aplica os conceitos técnico-econômicos da Escola Austríaca de Economia, provendo respaldo diante das características do dinheiro, tão bem como as funções da moeda. Foi apresentado o resultado da comparação de suas características ao papel-moeda e ao ouros por Fernando Ulrich.

Por fim, foi atuado na experimentação educacional da implementação de um sistema de *blockchain*, que abstrai os conceitos base do *Bitcoin*, permite a sua manipulação via requisições e exibe as classes presentes da corrente no navegador. Foram expostas todas as estruturas geradas neste experimento, seus atributos e suas funções diante da rede.

Trabalhos Futuros

Este projeto de *blockchain*, concebido com foco educacional e exploratório tanto da linguagem de programação Rust quanto da arquitetura de *blockchains*, abriu diversas possibilidades para melhorias e novas direções de desenvolvimento. Destacamos áreas de pesquisa e aprimoramento que poderão expandir as funcionalidades e aplicações práticas dessa arquitetura:

Aprimoramento do algoritmo de *Hashes* - Devido ao viés educativo foi utilizado de algoritmos de geração de *Hashes* simplistas. Utilizando poucos atributos das classes em questão resulta a criação de *Hashes* pouco complexos, o que impacta diretamente na flexibilidade da aplicação. Sendo assim abrindo margem para o retrabalho e aprimoramento do mesmo.

Otimização e Aprimoramento do Código Rust - Por conta do caráter exploratório do projeto diante da linguagem de baixo nível, há uma vasta gama de oportunidade para otimização e correções ao código escrito no nosso projeto. Dada a progressão da maturidade dos autores na linguagem, é esperada a constante manipulação da documentação do código e aprimoramento das estruturas apresentadas previamente. Este projeto exibe a visão de adequação para maior profundidade e semelhança ao algoritmo do *Bitcoin*, de acordo com a especialização dos autores no que se diz respeito a conhecimentos de criptografia, escalabilidade e segurança da informação.

Implementação de um Sistema de Assinatura Criptográfica - Conforme a estrutura da *blockchain* adquire maior robustez, é visível a abertura do acesso à rede a partir de assinaturas de chave privada e pública, permitindo que seus usuários crie e assine suas transações.

Expansão para Contratos Inteligentes - Uma das principais extensões possíveis para este projeto é a implementação de contratos inteligentes, que permitem a execução automatizada de contratos com base em condições predefinidas. Inspirado no modelo de contratos inteligentes introduzido por *Ethereum* (BUTERIN, 2013), o desenvolvimento de uma camada de *smart contracts* em Rust proporcionaria uma maior funcionalidade e flexibilidade à blockchain.

Aplicações Educacionais e Simuladores de Economia Digital - A proposta deste projeto inicialmente se tratava da possibilidade do desenvolvimento de um simulador de economia digital, onde estudantes e pesquisadores poderiam experimentar com transações, contratos e políticas econômicas diretamente na *blockchain*. Desenvolver integrações com interfaces amigáveis e *dashboards* que visualizem dados econômicos em tempo real poderia enriquecer o aprendizado e trazer novas oportunidades para a educação em economia digital e finanças descentralizadas. Embora ainda não tenhamos alcançado esta funcionalidade, este projeto ainda oferece esta finalidade como trabalho futuro.

Aprimoramento e Comportamento Similar a Outros Criptoativos - 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. Assim gerando a margem do desenvolvimento apoiado-se a novos criptoativos, conforme possam cumprir melhor as funções deste projeto.

Considerações Finais

Esses trabalhos futuros apresentam um roteiro para a evolução desta arquitetura de blockchain em Rust. O desenvolvimento dessas novas funcionalidades e a pesquisa contínua na área contribuirão para o avanço de novos projetos, permitindo que ultrapassem o ambiente acadêmico e ofereçam soluções inovadoras para desafios do mundo digital. Dessa forma, o projeto não apenas se tornará uma ferramenta educacional sólida para o estudo de economia no contexto da Web 3.0 e das finanças descentralizadas.

Particularmente, eu gostaria de prestar meus agradecimentos ao Professor Marc Antonio Vieira de Queiroz e ao Professor Orientador Mario Henrique Akihiko da Costa Adaniya pela sugestão de conteúdo, suporte e orientação pelo decorrer deste projeto.

Dedico este trabalho à minha noiva Lauren e ao leal GRUPP.

Liberdade é um dever.

REFERÊNCIAS

Actix Web Contributors. *Actix Web Documentation*. 2024. Accessed: 2024-10-26. Disponível em: <https://actix.rs/docs/>. 12

AUER, R.; CLAESSENS, S. Regulating cryptocurrencies: Assessing market reactions. *BIS Quarterly Review*, 2018. 6

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, 18

BöHM-BAWERK, E. v. *Capital and Interest*. [S.l.]: Macmillan, 1884–1889. 10

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>. 6

Jacob Lindahl (GeekLaunch). *Blockchain in Rust*. 2019. YouTube. Accessed: 2024-10-26. Disponível em: <https://www.youtube.com/playlist?list=PLwnSaD6BDfXL0RiKT_5nOIdxTxZWpPtAv>. 12

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. 12, 14

MISES, L. V. *The theory of money and credit*. [S.l.]: Oxford University Press, 1914. 10

NAKAMOTO, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. <https://bitcoin.org/bitcoin.pdf>. 4, 12, 13

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. maio 2009. Disponível em: <http://www.bitcoin.org/bitcoin.pdf>. 5, 7, 8, 9

Rust Project Developers. *Learn Rust Programming Language*. 2024. Accessed: 2024-10-26. Disponível em: <https://www.rust-lang.org/learn>. 12

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. 4

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>. 10, 11, 12

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>. 2

ZOHAR, A. Bitcoin: under the hood. *Communications of the ACM*, ACM New York, NY, USA, v. 58, n. 9, p. 104–113, 2015. 6