CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE INDAIATUBA
CURSO DE TECNOLOGIA EM REDES DE COMPUTADORES

VINICIUS MOTA NEVES

BLOCKCHAIN: A REVOLUÇÃO TECNOLÓGICA POR TRÁS DO BITCOIN

INDAIATUBA/SP
2025

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE INDAIATUBA
CURSO DE REDES DE COMPUTADORES

VINICIUS MOTA NEVES

BLOCKCHAIN: A REVOLUÇÃO TECNOLÓGICA POR TRÁS DO BITCOIN

Trabalho de Graduação apresentado como pré-requisito para a conclusão do Curso Superior de Tecnologia em Redes de Computadores, da Faculdade de Tecnologia de Indaiatuba, elaborado sob a orientação do Prof. Samuel dos Santos.

INDAIATUBA/SP
2025

AGRADECIMENTOS

Agradeço a Deus primeiro lugar, que iluminou o meu caminho e permitiu-me chegar até aqui.

Agradeço aos meus professores, pelo conhecimento compartilhado, pela orientação e pela motivação nessa trajetória.

Agradeço a minha mãe, que me ajudou a enfrentar os desafios e sempre me apoiou.

DEDICATÓRIA

Dedico este trabalho a minha família, aos meus colegas, ao meu orientador e a meus professores pelos ensinamentos, apoio e incentivo ao longo desta jornada.

RESUMO

O Bitcoin surgiu em 2008 em meio a uma grande crise financeira como uma inovação tecnológica baseada em *blockchain*, propondo um sistema financeiro descentralizado, seguro, transparente e imutável. Desde então, a tecnologia evoluiu significativamente, consolidando-se como uma alternativa segura e prática, contribuindo para que sua moeda escassa se tornasse uma reserva de valor e um ativo financeiro amplamente adotado. Este trabalho tem como objetivo geral analisar a tecnologia e mecanismos da rede Bitcoin buscando apresentar uma visão técnica e detalhada, explicando sua estrutura, funcionamento, inovações e problemas enfrentados, além das características do ativo Bitcoin. Para isso, será feita uma pesquisa qualitativa, baseada em revisão bibliográfica e análise documental dos principais trabalhos da área. Como parte do trabalho, foi desenvolvido um simulador gráfico simplificado de uma blockchain, com o objetivo de ilustrar, de forma didática, os principais componentes e operações de funcionamento da rede. Espera-se que através das análises realizadas, seja possível compreender, o funcionamento da rede Bitcoin e de seus mecanismos, os principais marcos de sua trajetória, suas inovações tecnológicas e seu impacto no cenário econômico global.

Palavras-chave: Bitcoin. Blockchain. Descentralização. Escalabilidade.

ABSTRACT

Bitcoin emerged in 2008 amid a major financial crisis as a technological innovation based on blockchain, proposing a decentralized, secure, transparent, and immutable financial system. Since then, the technology has evolved significantly, establishing itself as a safe and practical alternative, contributing to its scarce currency becoming a store of value and a widely adopted financial asset. This work aims to analyze the technology and mechanisms of the Bitcoin network, presenting a technical and detailed overview that explains its structure, operation, innovations, and challenges, as well as the characteristics of the Bitcoin asset. To achieve this, a qualitative study will be conducted, based on a literature review and documentary analysis of key works in the field. As part of this research, a simplified graphical blockchain simulator was developed with the goal of illustrating, in a didactic way, the main components and operational processes of the network. It is expected that, through the analyses carried out and the developed tool, it will be possible to understand the functioning of the Bitcoin network and its mechanisms, the main milestones in its history, its technological innovations, and its impact on the global economic landscape.

Keywords: Bitcoin, Blockchain, Decentralization, Store of Value, Scalability.

LISTA DE FIGURAS

LISTA DE SIGLAS

BTC	Bitcoin
POW	*Proof of Work*
POS	*Proof of Stake*
MEMPOOL	*Memory Pool*
ETF	*Exchange Traded Fund*
MB	*Megabyte*
CPU	*Central Processing Unit*
SAT	*Satoshi*
TPS	Transação por Segundo
P2P	Ponto a Ponto
DEFI	*Decentralized Finance*
TWH	TeraWatt-hora

SUMÁRIO

1 INTRODUÇÃO

O sistema financeiro tradicional, dominado por bancos e outras instituições centrais, apresenta diversas fragilidades decorrentes de sua estrutura centralizada. Problemas como falta de transparência, falhas sistêmicas, manipulação cambial e risco moral têm historicamente contribuído para crises financeiras ao redor do mundo. A Grande Depressão de 1929 (TERMIN, 1994) e a crise financeira de 2008 são exemplos emblemáticos dessas vulnerabilidades, evidenciando a fragilidade dos bancos diante de eventos econômicos extremos e a influência de políticas monetárias na estabilidade do sistema. A crise financeira de 2008 expôs falhas nos mecanismos regulatórios e na conduta ética das instituições financeiras, destacando como incentivos mal estruturados e a expectativa de apoio governamental favoreceram comportamentos de risco por parte dos executivos. (MENG; YUAN; CHEN, 2021)

Foi nesse contexto de instabilidade e desconfiança no sistema financeiro tradicional que surgiu o Bitcoin. Em 31 de outubro de 2008, Satoshi Nakamoto publicou o whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System", descrevendo um sistema de dinheiro eletrônico descentralizado, seguro e transparente, eliminando a necessidade de intermediários financeiros. Baseado em blockchain e no mecanismo de consenso Proof of Work (PoW), o Bitcoin introduziu um novo modelo monetário, onde qualquer participante da rede poderia verificar transações, garantindo um registro imutável e resistente à censura. Desde sua implementação em 2009, a tecnologia se consolidou como uma alternativa ao sistema financeiro tradicional, proporcionando maior autonomia financeira aos usuários e proteção contra políticas econômicas arbitrárias.

Conforme o Bitcoin ganhou adoção, desafios técnicos emergiram, sendo a escalabilidade um dos mais debatidos. A rede Bitcoin processa apenas cerca de sete transações por segundo, e o tempo médio de confirmação de um bloco é de aproximadamente 10 minutos, o que pode ser um entrave para transações cotidianas. Para mitigar esse problema, surgiram soluções como a Lightning Network, que permite transações instantâneas e de baixo custo ao operar fora da

blockchain principal, mantendo a segurança e a descentralização. Essas melhorias possibilitaram a ampliação do uso do Bitcoin além da reserva de valor, tornando-o uma opção viável para micropagamentos.

Paralelamente, a evolução da blockchain trouxe novas inovações, como a criação da Ethereum em 2015, que introduziu contratos inteligentes (smart contracts) e expandiu o uso da tecnologia para além das transações financeiras. O surgimento de aplicativos descentralizados (dApps) e soluções como rollups e sidechains buscou resolver o chamado "trilema da blockchain", que equilibra segurança, descentralização e escalabilidade. Enquanto outras redes exploravam essas soluções, o Bitcoin manteve um enfoque conservador em sua estrutura, priorizando a segurança e a imutabilidade, consolidando-se como um ativo escasso e confiável para preservação de valor a longo prazo.

Nos últimos anos, o Bitcoin passou a ser amplamente adotado por investidores institucionais, consolidando-se como uma reserva de valor digital. O sucesso dos ETFs e o acúmulo de Bitcoin por parte de empresas e governos ajudam a evidenciar essa tendência. Atualmente, o Bitcoin ocupa uma posição entre os ativos mais valiosos do mundo, reforçando sua narrativa como "ouro digital".

Apesar dessa ascensão, o entendimento técnico sobre o Bitcoin ainda é limitado por grande parte do público, o que gera ceticismo e desinformação. Muitas críticas decorrem da falta de conhecimento sobre princípios da tecnologia e de como ela funciona. Dessa forma, este trabalho tem como objetivo apresentar uma visão técnica e detalhada sobre o Bitcoin, explicando sua estrutura, funcionamento e inovações. Além disso, por meio de uma análise histórica, serão abordados os desafios enfrentados pela rede, as soluções desenvolvidas ao longo do tempo e os impactos dessa tecnologia na sociedade e na economia global.

O estudo também visa abordar o papel que o Bitcoin vem assumindo no cenário financeiro, discutindo as características que fazem com que ele seja encarado como reserva de valor, meio de troca e um meio viável para liquidar grandes transações internacionais além da sua crescente adoção institucional. Espera-se que, ao compreender melhor o funcionamento da tecnologia e as

características do ativo, este trabalho contribua para a desmistificação do tema e forneça uma base sólida para que os leitores avaliem o Bitcoin de forma fundamentada e objetiva.

2 REVISÃO DA LITERATURA/BIBLIOGRÁFICA

2.1 Cadeia de assinaturas digitais

Nakamoto(2008) descreve a rede Bitcoin como um sistema que utiliza uma rede peer-to-peer baseados em provas criptográficas e assinaturas digitais, para permitir que os pagamentos sejam enviados diretamente de um remetente para um destinatário, sem passar por uma instituição financeira, as transações são validadas de forma distribuída por meio do consenso dos nós participantes da rede. Essa estrutura descentralizada é capaz de realizar transações de forma efetiva com segurança e autonomia, mitigando os riscos associados à centralização, como censura e falhas sistêmicas.

As assinaturas digitais são um dos principais mecanismos que viabilizam a confiança em ambientes digitais. Elas funcionam de maneira semelhante a uma assinatura manuscrita em um contrato, mas com um nível de segurança infinitamente maior, baseado em criptografia .

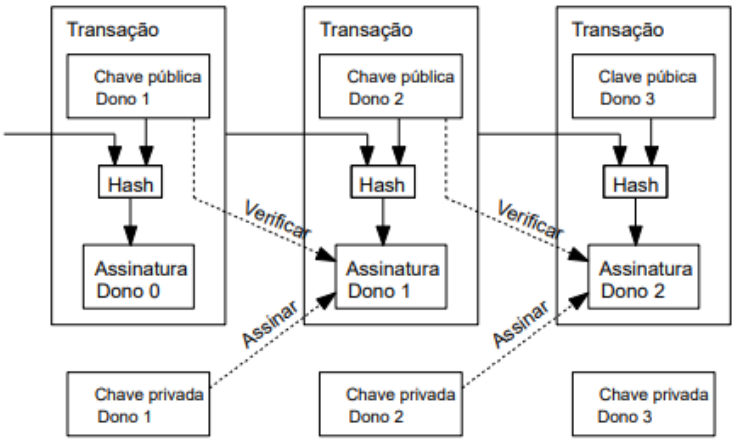
De acordo com Vieira (2011), “a primeira forma de criptografia foi a Simétrica, desempenhava o papel de cifrar ou ocultar dados sigilosos. Posteriormente surgiu a criptografia assimétrica, também conhecida como chave pública e chave privada. A criptografia provê recursos para garantir os serviços de autenticação, integridade, confidencialidade e Irretratabilidade.”

No protocolo do bitcoin, o acesso às moedas é controlado por pares de chaves da criptografia assimétrica, em que a chave pública é usada para receber bitcoins e a chave privada para assinar transações para gastá-los. Uma assinatura gerada com a chave privada pode ser validada sem que a chave seja revelada.

De acordo com Nakamoto (2008) “Definimos uma moeda eletrônica como uma cadeia de assinaturas digitais. Cada proprietário transfere a moeda para o próximo assinando digitalmente um *hash* da transação anterior e a chave pública do

próximo proprietário, e adicionando isso ao final da moeda. Um beneficiário pode verificar as assinaturas para confirmar a cadeia de propriedade.”

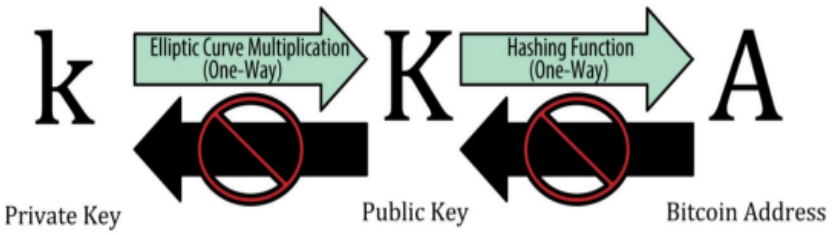
Figura 1: Assinaturas digitais.



Fonte: Nakamoto Satoshi 2008.

Segundo Figueiredo (2020) “No Bitcoin gera-se uma chave privada k, que consiste em um grande número aleatório, e então computa-se a chave pública correspondente K, usando-se multiplicação de curvas elípticas. Produz-se um endereço bitcoin computando-se o hash SHA256 a partir de K e então o hash RIPEMD160 a partir do resultado.”

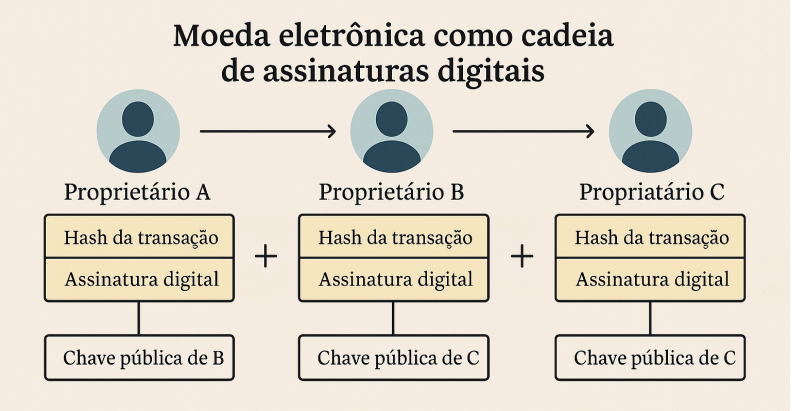
Figura 2: Endereços Bitcoin.



Fonte: Antonopoulos Andreas 2017.

A cadeia de assinaturas digitais, compõe um registro de transferências anteriores em cada moeda que é vinculada por assinaturas digitais, estas comprovam que a moeda foi passada de forma legítima de um proprietário para o outro. Quando o proprietário desejar transferir a moeda, ele terá que criar uma assinatura digital utilizando sua chave privada, garantindo que só ele poderá autorizar a transação, o hash da transação anterior será incluído, criando uma conexão entre a nova transação e a cadeia anterior e também será incluída a chave pública do próximo proprietário. Esses vínculos acabam criando uma cadeia inquebrável de transações.

Figura 3: Transferências



Fonte: Inteligência artificial, 2025.

Contudo, apenas a verificação de assinaturas digitais entre remetente e destinatário não é suficiente para evitar problemas como o gasto duplo, onde uma mesma moeda poderia ser enviada para mais de uma pessoa. Para resolver esse desafio, é necessário garantir que exista um registro cronológico e público das transações, impedindo que transações conflitantes sejam aceitas. É nesse ponto que entra a cadeia de blocos (blockchain). que agrupa as transações realizadas em blocos ordenados de forma temporal.

2.2 Blockchain

A Blockchain é uma tecnologia que agrupa transações dentro de blocos conectados de forma temporal através de hashes criptográficos, gerando uma cadeia de registros ordenada e imutável.

De acordo com Lago(2017):

“1. Todas as transações realizadas nos últimos minutos são agrupadas em um único bloco;

2. Esse único bloco é distribuído por toda a rede da blockchain para ser validado;

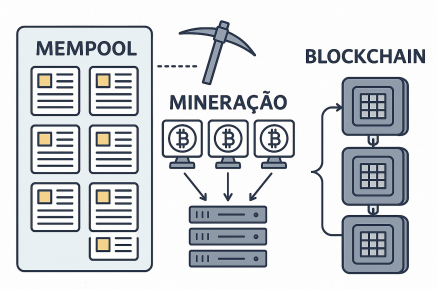
3. Usuários da rede com computadores utilizam algoritmos para validar o bloco, e recebem recompensas a cada sucesso. Esses usuários são chamados de mineradores;

4. O bloco validado recebe uma marcação temporal e é adicionado no final da lista.”

Para que uma transação seja efetivamente validada, ela precisa ser inserida em um bloco que por sua vez terá que ser minerado (adicionado a cadeia). Mas para que isso aconteça, antes as transações pendentes passam por um pool de memória (frequentemente abreviado como *mempool*), onde aguardam a formação do próximo bloco onde serão incluídas. Segundo Albrecher e Goffard (2024), as transações pendentes são armazenadas no *pool* de memória, onde aguardam confirmação, formando assim uma fila.

A taxa de transação está intimamente relacionada ao congestionamento do *mempool*, o custo médio gira em torno de 10 a 30 sat/vByte, uma transação simples ocupa cerca de 150 vBytes, porém um bloco possui tamanho fixo de 1Mb (BEVILACQUA, 2018), o que limita a quantidade de transações que ele pode conter, então quanto mais cheio o *mempool estiver,* mais caro o custo do sat/vByte ficará, pois os mineradores darão prioridade às transações com taxas maiores.

Figura 4: Mempool.



Fonte: Inteligência artificial, 2025.

Para garantir a validade e a integridade desses blocos, o whitepaper introduz o conceito de um mecanismo de consenso, que é a maneira como a blockchain valida e registra novas transações na blockchain. O método de prova de trabalho (Proof of Work) é utilizado para assegurar que as transações sejam verificadas e confirmadas de maneira confiável, prevenindo fraudes, duplicação de gastos e imutabilidade.

De acordo com Nakamoto(2008), “a cadeia de prova de trabalho é um registro público de transações que rapidamente se torna computacionalmente impraticável de alterar, desde que os nós honestos controlem a maioria do poder de CPU”

Na blockchain, cada bloco é validado por meio do Proof-of-Work, que consiste na resolução de um cálculo matemático complexo por parte dos mineradores. Esse cálculo tem como finalidade encontrar um "*nonce*" que gerará um *hash* específico para o bloco. Quando o bloco é validado, ele é aceito pela cadeia.

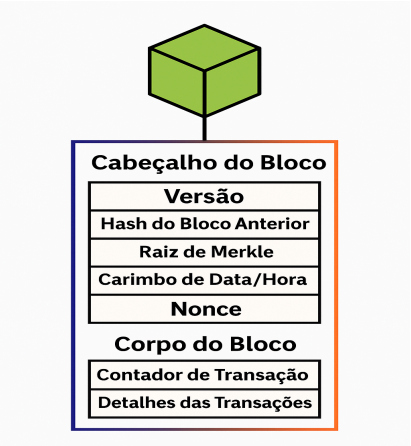
De acordo com Lago(2017), “uma função *hash* pode transformar qualquer informação em uma lista de letras e números que aparenta ser aleatória.”

Figura 5: Hash Criptográfico.

Fonte:Jansen, 2022.

Cada novo bloco da blockchain utiliza as informações de índice do bloco, hash do bloco anterior, dados do bloco, data e hora, e um número chamado de “nonce” como entrada para a sua função hash.

Figura 6: Conteúdo do Bloco.



Fonte: Autor, 2025.

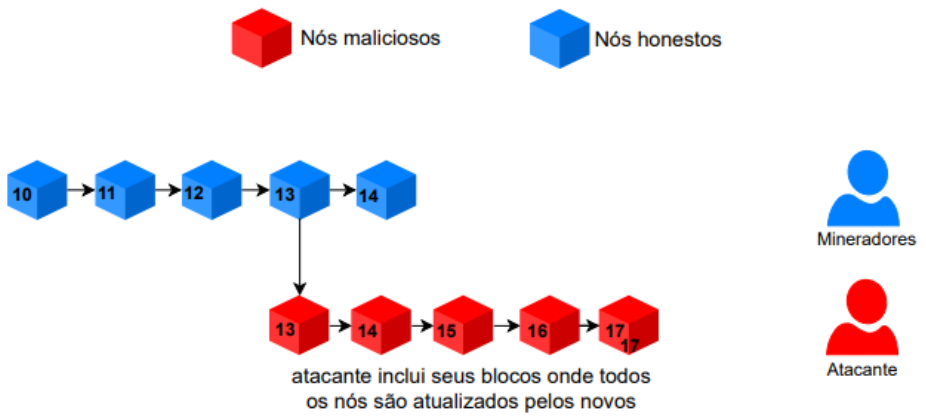
Segundo Lago (2017), “caso o hash gerado por essa entrada seja válido, o bloco é aceito como válido e transmitido para todos os membros da rede distribuída; caso o hash não seja válido, o número “nonce” é alterado por um novo valor. Esse processo é repetido até que um número “nonce” capaz de validar o bloco seja encontrado. Esse processo é chamado de mineração de bloco”

Para que esse mecanismo de validação fosse sustentável foi estabelecido um modelo de incentivo onde o nó minerador que encontrar o nonce do bloco é recompensado. Segundo Pereira (2025) “o primeiro a encontrar a solução válida do problema matemático, tem o direito de adicionar um novo bloco à blockchain, sendo recompensado com uma quantidade fixa (block reward) da criptomoeda minerada, além das taxas de transações do bloco.”

A segurança da blockchain se dá pelo consenso da maioria, ou seja, para um atacante conseguir modificar os registros da blockchain e validar a cadeia adulterada, ele sozinho precisaria ter a maior parte do poder computacional da rede. Com 51% do poder de mineração, o atacante pode explorar e modificar a cadeia de blocos, eliminando ou inserindo transações (Kreutz, 2024). Além disso, para alterar um bloco já validado, o atacante precisaria refazer o processo de Proof of Work de todos os blocos subsequentes, criando uma segunda cadeia, que seria rejeitada pela rede caso não superasse o poder computacional dos mineradores honestos.

Segundo Figueiredo (2020): “Quando uma transação é incluída em um bloco válido da cadeia, é dito que ela possui uma confirmação. Cada bloco adicionado posteriormente é uma confirmação adicional. Por convenção, após seis confirmações a transação é considerada irrevogável, pois o esforço computacional para invalidar e recalcular seis blocos seria absurdo.”

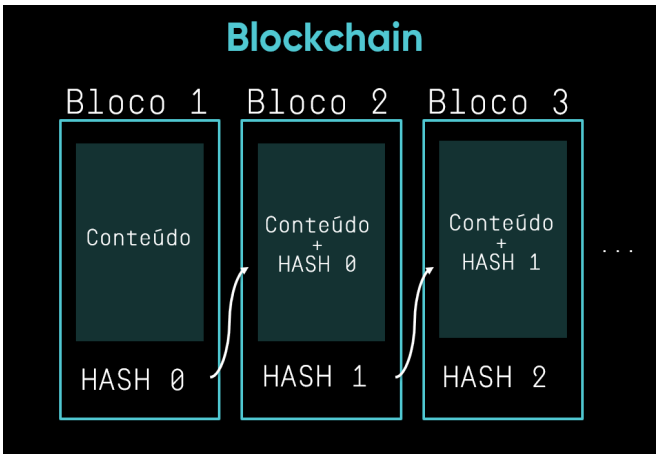
Figura 7: Ataque 51%.



Fonte: Diego Kreutz, 2024.

Além do bloco com os registros alterados o atacante também precisaria refazer a prova de trabalho de todos os blocos seguintes até o atual para que sua cadeia fosse aceita, pois mudando um único dado dentro do bloco o seu hash será alterado por completo e no cabeçalho de um bloco sempre haverá o hash do bloco anterior, sendo assim, alterar um único valor dentro de um bloco, causaria discordâncias entre os hashes, quebrando o vínculo dele com o bloco subsequente o que faria com que a cadeia adulterada fosse rapidamente rejeitada.

Figura 8: Cadeia de blocos.



Fonte: Greyson Farias, 2022.

De acordo com Nakamoto(2008): “Para modificar um bloco passado, um atacante precisaria refazer a prova de trabalho desse bloco e de todos os blocos posteriores, além de alcançar e superar o trabalho realizado pelos nós honestos.”

Ou seja, digamos que os mineradores estejam trabalhando para minerar o bloco número 20 da cadeia e um atacante ou minerador queira alterar uma transação no bloco 8, ele teria que fazer a alteração e minerar todos os blocos do 8 até o 19 além do bloco 20, seriam gastos recursos de tempo, energia e processamento para minerar 13 blocos, porém o que torna isso impraticável é o fato de que ele precisaria fazer tudo isso antes de os outros mineradores criarem o bloco 20.

Figura 9: Imutabilidade.

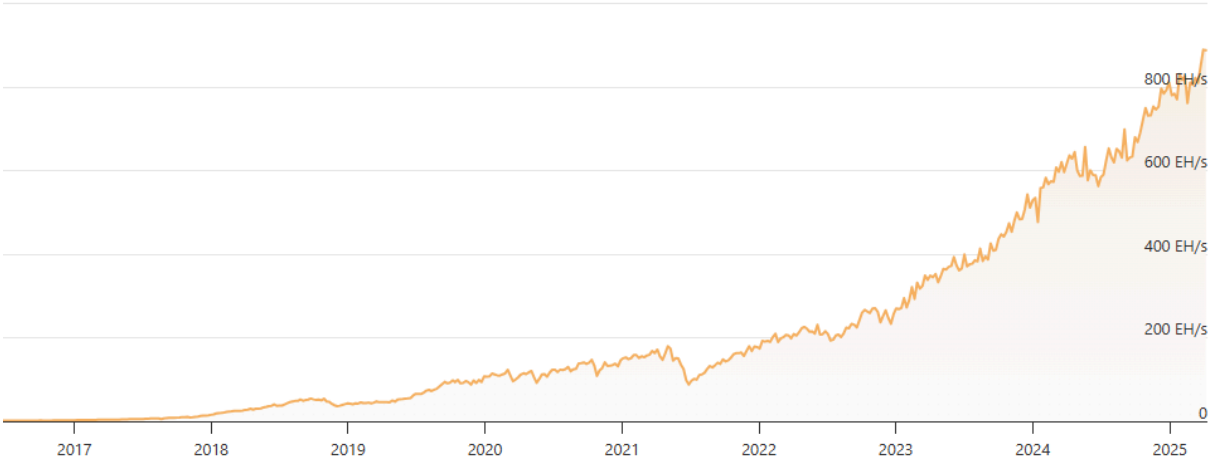
Fonte: FoxBit, 2023.

Existem diferentes contra-medidas que podem mitigar a possibilidade de um ataque de 51%. Segundo Kreutz (2024) “O ataque pode ser prevenido se evitarmos participar de pools de mineração formados por grupo de mineradores que possuem uma grande capacidade de mineração. Um segundo exemplo de contra-medida é desenvolver algoritmos de consenso que dificultem que poucas máquinas possam ter controle de mais de 50% da capacidade de geração de blocos. Por exemplo, podem ser utilizados algoritmos baseados em votação.”

Apesar do tema gerar debate e ser abordado em diversos trabalhos, não existe nenhum registro de que um dia houve um ataque de 51% na história da rede Bitcoin e a cada dia a probabilidade de acontecer diminui devido ao aumento do hashrate da rede o que a torna mais segura.

De acordo com Calzar (2023), “o hashrate de uma plataforma de mineração é o número de hashes que ela pode calcular por segundo. O hashrate combinado de uma rede de criptomoedas é a soma dos hashrate de todas as plataformas de mineração que estão em operação em um determinado período.”

Figura 10: Hashrate.



Fonte: CoinWarz, 2025.

Em outras palavras, o hashrate representa o poder computacional de todos os dispositivos de mineração conectados à rede juntos, sendo assim conforme o hashrate aumenta, mais segura a rede se torna pois também é aumentada a dificuldade de um único nó possuir 51% do poder computacional para realizar um ataque.

2.3 Redes de Segunda Camada

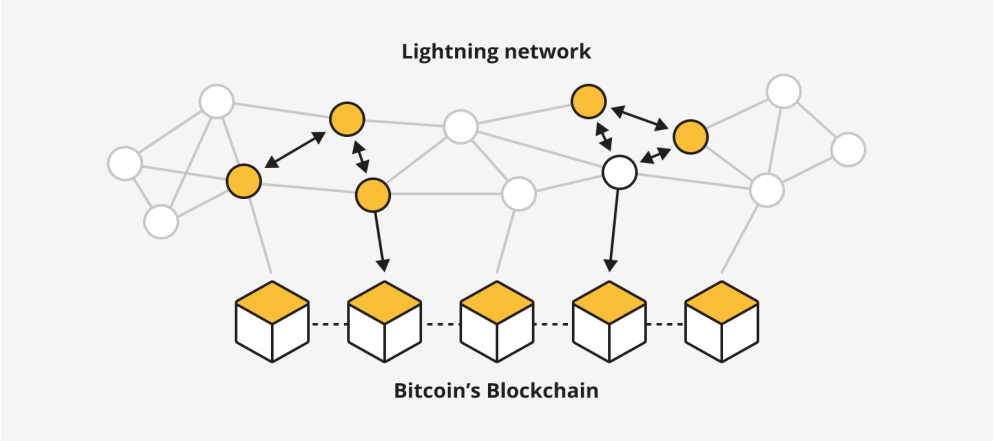
Um dos principais desafios com a tecnologia subjacente do Bitcoin é a escalabilidade, pois seu limite é de 7 transações por segundo, em comparação a rede de processamento de cartões de crédito da VISA lida rotineiramente com 2.000 transações por segundo e pode acomodar volumes de pico de até 10.000 transações por segundo. (SWAN, 2015)

Para resolver esse problema foram criadas as Off-Chain. De acordo com Machado(2024), “as “Off-Chains” surgiram pela necessidade de escalabilidade que Blockchains como o Bitcoin, necessitam para alcançar grandes volumes de ações na

rede. As Off-chains entregam melhor velocidade de transação com menos custo energético, podendo assim ser uma alternativa mais sustentável e rápida, sem ter que ser feita uma grande mudança na rede principal.”

Uma das principais soluções off-chain para o Bitcoin é a Lightning Network, uma rede de segunda camada que permite a criação de canais de pagamento fora da blockchain principal. Esses canais funcionam como “acordos” entre duas partes, permitindo a realização de transações instantâneas com baixas taxas. Apenas quando o canal é fechado, o saldo final é registrado na blockchain do Bitcoin.

Figura 11: Lightning Network.



Fonte: Furlan, 2025.

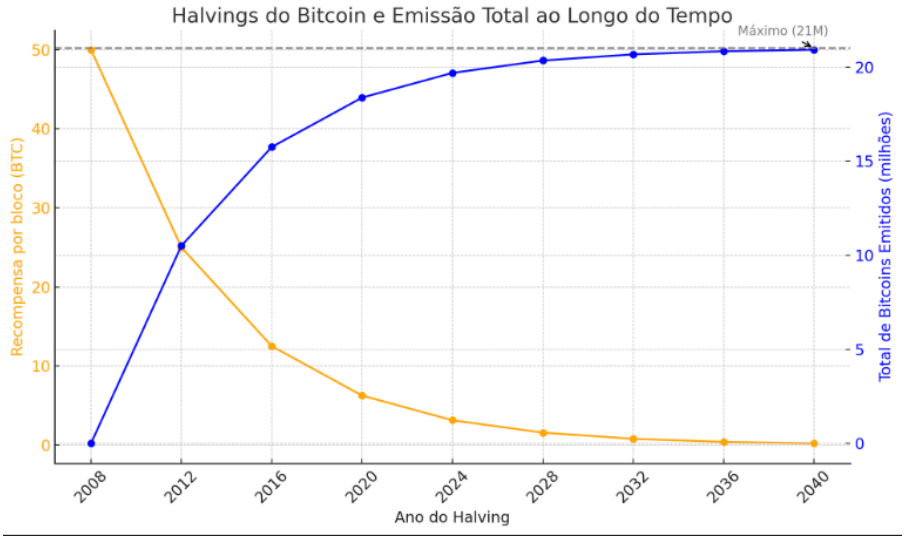
Esse modelo reduz significativamente a carga da rede principal, pois evita que cada transação precise ser validada e armazenada diretamente na blockchain. Como destacado por POON e DRYJA (2016) “a Lightning Network possibilita micropagamentos escaláveis, mantendo a segurança da rede subjacente ao mesmo tempo que melhora sua eficiência e usabilidade.”

2.4 Características econômicas do Bitcoin

Além de seu funcionamento técnico, o Bitcoin possui características econômicas que influenciam diretamente sua proposta de valor no mercado. Um dos

principais aspectos é sua escassez programada, que o diferencia das moedas fiduciárias, as quais podem ser emitidas em grandes quantidades por bancos centrais. O protocolo Bitcoin define um fornecimento máximo de 21 milhões de unidades, sendo emitidas de forma controlada por meio do processo de mineração. A cada aproximadamente quatro anos ocorre o chamado *halving*, que reduz pela metade a recompensa concedida aos mineradores por bloco minerado. Este mecanismo garante que a emissão de novos bitcoins diminua ao longo do tempo, reforçando sua característica deflacionária e escassa (ANTONOPOULOS, 2017).

Figura 12: Escassez Programada.



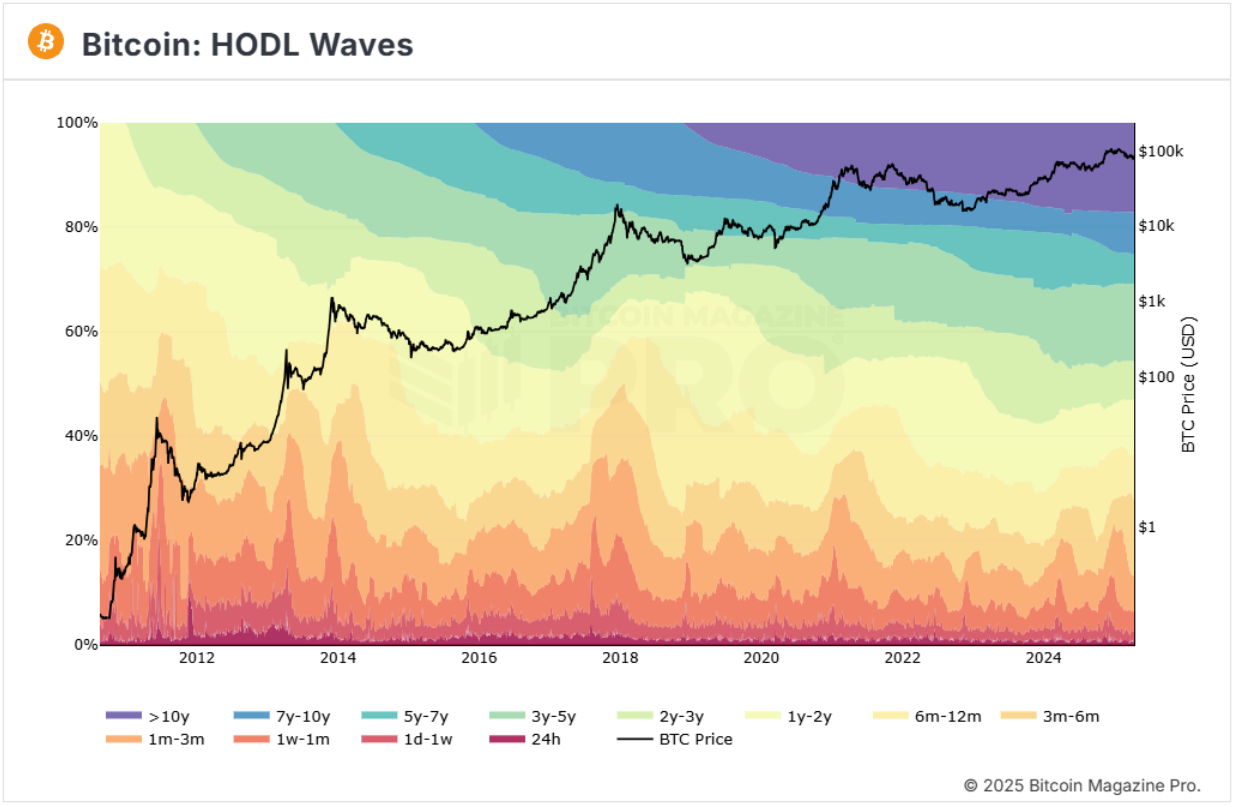
Fonte: Autor, 2025.

Essa escassez, combinada com sua natureza descentralizada e resistência à censura, contribui para que o Bitcoin seja cada vez mais visto como uma reserva de valor, especialmente em contextos de instabilidade econômica ou inflação elevada. Ao contrário de sistemas tradicionais, que dependem da confiança em instituições centrais, o Bitcoin oferece uma alternativa baseada em regras matemáticas previsíveis e transparência. Isso atrai investidores que buscam proteção de patrimônio no longo prazo, mesmo que a rede não ofereça, em sua forma atual, a escalabilidade necessária para se tornar uma plataforma global de micropagamentos (REYNA et al., 2018).

Um dos indícios desse comportamento pode ser observado no crescente número de detentores de longo prazo (Long-Term Holders). De acordo com Chen(2024), “um fator que apresenta um padrão fortemente correlacionado com o preço do Bitcoin é o número de Bitcoins possuídos por detentores de longo prazo.”

Esses usuários são caracterizados por armazenar seus bitcoins por períodos superiores a seis meses, evidenciando uma postura de retenção ao invés de movimentação frequente. Na **Figura 13** podemos ver a correlação do crescimento dos Long-Term Holders com o valor do Bitcoin como apontado por Chen.

Figura 13: Long-Term Holders.



Fonte: BitcoinMagazine, 2025.

A Figura apresentada acima, além de ilustrar essa tendência de crescimento dos Long-Term Holders e a correlação anteriormente mencionada, também nos mostra que mais de 50% dos Bitcoins não são movimentados a pelo menos 2 anos, o que contribui para o choque de demanda.

3 MATERIAIS E MÉTODOS

3.1 Tipo de Pesquisa

Este trabalho adota uma abordagem qualitativa e exploratória, voltada para a compreensão dos fundamentos técnicos da tecnologia blockchain e a evolução do Bitcoin ao longo do tempo. A natureza qualitativa permite analisar documentos, artigos e dados históricos sob uma perspectiva interpretativa, enquanto o caráter exploratório é justificado pelo aprofundamento em tecnologias emergentes e suas implicações para a área de redes e sistemas distribuídos.

3.2 Fontes de Dados

Foram utilizados dados e informações secundárias, obtidos por meio de whitepapers, artigos científicos, livros especializados, sites técnicos, portais de métricas (como Coinwarz e Glassnode), além de materiais acadêmicos disponíveis em bases como Google Scholar (Google Acadêmico). As fontes escolhidas abordam aspectos técnicos, históricos e funcionais relacionados à rede Bitcoin, à tecnologia blockchain e às soluções propostas para seus desafios.

3.3 Método de Coleta

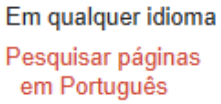
A coleta de informações foi realizada por meio de revisão bibliográfica e documental, com foco em textos que abordam diretamente sobre o funcionamento da rede blockchain, mas também trabalhos que abordam especificamente sobre um recurso, conceito ou mecanismo que seja utilizado na rede. O Google Acadêmico foi a principal fonte de busca onde foram feitas pesquisas orientadas por palavras-chave específicas como “Blockchain”, “hash criptográfico”, “Proof-of-work” e “mineração” para encontrar trabalhos que abordassem diretamente sobre esses assuntos, conforme é visto na figura abaixo.

Figura 14: Palavras-chave utilizadas no Google Acadêmico.

Fonte: Autor, 2025.

Após a inserção das palavras-chave, aplicou-se o filtro de Idioma para publicações em Português, uma vez que o trabalho prioriza fontes no idioma nacional, conforme mostra a **Figura 15**.

Figura 15: Filtro de Idiomas do Google Acadêmico.



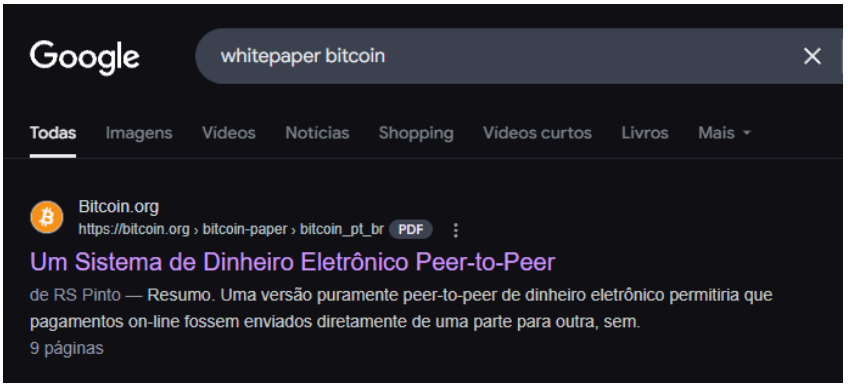
Fonte: Autor, 2025.

Aplicando esses critérios os estudos retornados eram então avaliados quanto a sua relevância e forma de abordagem em relação ao tema pesquisado.

O autor também consumiu como fonte, trabalhos que eram comumente citados como referência nos estudos analisados, levando em consideração a relevância que aqueles trabalhos demonstraram ter. Seguindo esse critério também foram selecionados estudos de outras línguas.

Também foram utilizados documentos técnicos oficiais (*Whitepaper*) de redes abordadas nesse estudo, como o caso do Bitcoin e a Lightning Network, ambos obtidos por meio de pesquisas em fontes confiáveis na internet, principalmente no próprio Google.

Figura 16: Pesquisa de documentos oficiais.



Fonte: Autor, 2025.

3.4 Análise de Dados

A análise dos dados foi realizada de forma qualitativa, com base em uma interpretação crítica do conteúdo encontrado nas fontes consultadas, priorizando trabalhos que apresentassem:

- Abordagem técnica clara sobre o funcionamento da rede Bitcoin e da tecnologia blockchain;
- Relevância científica, medida pelo grau de citação ou pela publicação em veículos reconhecidos;
- Atualidade, especialmente no que diz respeito aos desafios técnicos recentes, como a escalabilidade, e soluções como a Lightning Network;
- Contribuições significativas para o entendimento da evolução da rede Bitcoin, seja do ponto de vista técnico ou conceitual.

Os documentos selecionados foram submetidos a uma leitura analítica, buscando identificar padrões, conceitos recorrentes, marcos históricos e divergências interpretativas entre os autores. Esse processo permitiu reunir evidências que fundamentassem a discussão dos principais marcos evolutivos da rede Bitcoin, os desafios enfrentados ao longo do tempo, e as soluções técnicas propostas.

Além disso, foram incluídas no trabalho análises contextuais sobre o uso atual do Bitcoin como reserva de valor, mesmo que isso não estivesse nos objetivos originais da rede, apontando para uma reinterpretação de seu propósito inicial. Essa mudança de papel também foi influenciada pelas características econômicas do ativo, as quais também foram abordadas no trabalho.

Por fim, o simulador desenvolvido foi utilizado como apoio didático e técnico, reforçando de forma prática o entendimento dos conceitos teóricos abordados. Ainda que nem todos os tópicos discutidos nos resultados estejam representados no simulador, ele cumpre a função de validar parte dos conhecimentos aplicados, especialmente no que diz respeito à estrutura básica de funcionamento da blockchain e do mecanismo de consenso por Proof-of-Work.

3.5 Validação dos Resultados

A validação dos resultados foi realizada por meio de uma abordagem híbrida. Conceitos técnicos descritos na fundamentação teórica foram parcialmente validados com o apoio de um simulador de blockchain, desenvolvido especificamente para este trabalho. Já os resultados relacionados ao comportamento atual da rede Bitcoin e sua mudança de propósito foram validados por meio de revisão bibliográfica e análise de dados de mercado. Dessa forma, a combinação entre artefato técnico e embasamento teórico permitiu uma validação ampla dos pontos discutidos.

3.6 Desenvolvimento de Artefato Técnico

Como parte da validação conceitual dos conteúdos abordados, foi desenvolvido um simulador gráfico em Python com interface construída utilizando a biblioteca Tkinter. O objetivo deste artefato é ilustrar, de forma didática, o funcionamento básico de uma blockchain, demonstrando o processo de geração de endereços, criação de transações, mineração de blocos e a estrutura da cadeia de blocos encadeados por seus respectivos hashes.

O simulador não busca representar com precisão todas as complexidades de uma rede como o Bitcoin, mas sim facilitar a compreensão prática dos principais conceitos relacionados ao tema. O código-fonte completo e o manual de utilização encontram-se nos Apêndices deste trabalho.

4 RESULTADOS E DISCUSSÃO

4.1 Evolução do Propósito do Bitcoin

Desde seu surgimento, a rede Bitcoin enfrenta limitações técnicas relacionadas à escalabilidade. Por operar com blocos de tamanho fixo (1MB) e intervalos médios de 10 minutos entre blocos, o sistema suporta cerca de 7 transações por segundo (TPS), o que é significativamente inferior a sistemas tradicionais de pagamento como Visa ou Mastercard. Esse gargalo técnico, somado ao aumento da demanda, fez com que taxas de transação elevadas e congestionamentos se tornassem frequentes em períodos de alto uso.

Além disso, o próprio *mempool* da rede (onde transações pendentes aguardam validação) pode ficar sobrecarregado, o que pressiona ainda mais as taxas, dificultando a utilização do Bitcoin para transações cotidianas de pequeno valor, como compra de um café ou pagamento de pequenas despesas.

4.1.1 Transição para reserva de valor: Motivações

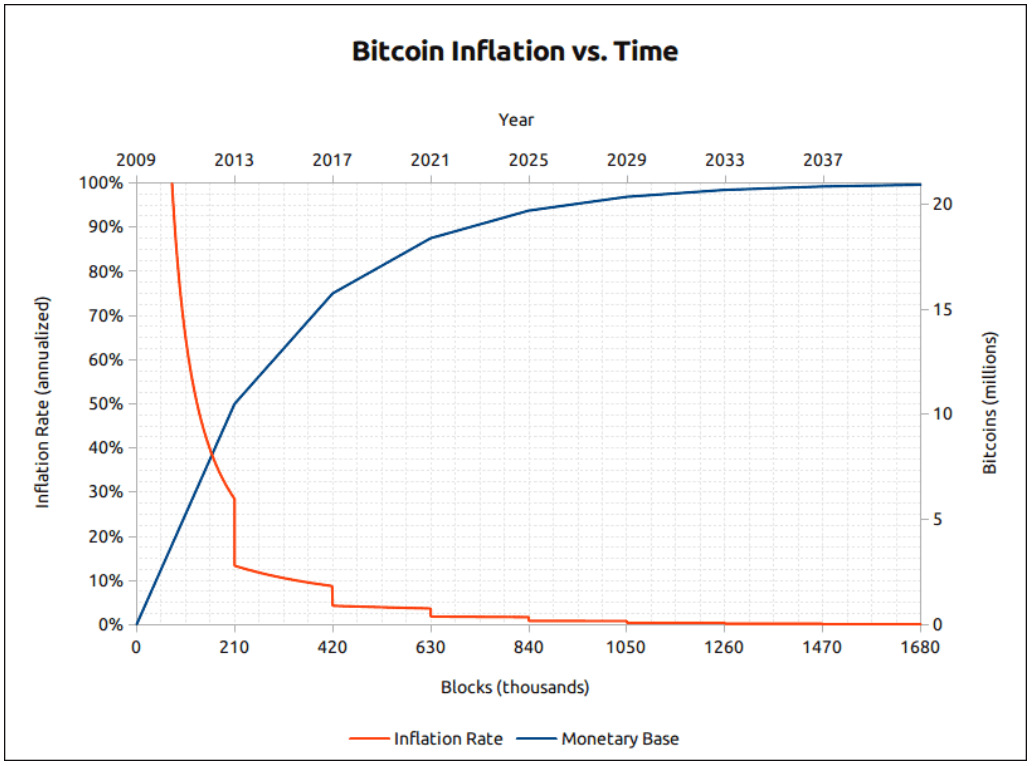
Apesar das limitações de escalabilidade, o Bitcoin passou por uma mudança em seu posicionamento prático e simbólico: de uma moeda digital voltada para pagamentos, ele passou a ser visto e utilizado principalmente como um ativo de reserva de valor, similar ao ouro digital. Diversos fatores contribuíram para essa transição:

- Oferta limitada a 21 milhões de unidades estabelecida em seu código, o que garante escassez e elimina a possibilidade de inflação monetária descontrolada, comum em moedas fiduciarias.
- Eventos de halving que ocorrem aproximadamente a cada quatro anos, diminuindo a emissão de novos BTCs e aumentando a percepção de escassez. Esse mecanismo continuará até que o limite máximo de 21 milhões

de bitcoins seja atingido, o que está previsto para ocorrer por volta do ano 2140.

- Descentralização e resistência à censura, tornando-o atrativo em contextos políticos ou econômicos instáveis, especialmente em países com hiperinflação ou controle de capitais.
- Desconfiança em moedas fiduciárias e bancos centrais, especialmente após crises econômicas como a de 2008, que motivou a criação do próprio Bitcoin.
- Adoção institucional por grandes fundos de investimento, bancos e ETFs, que reforçaram a imagem do Bitcoin como um instrumento de proteção de patrimônio no longo prazo.

Figura 17: Inflação do Bitcoin.



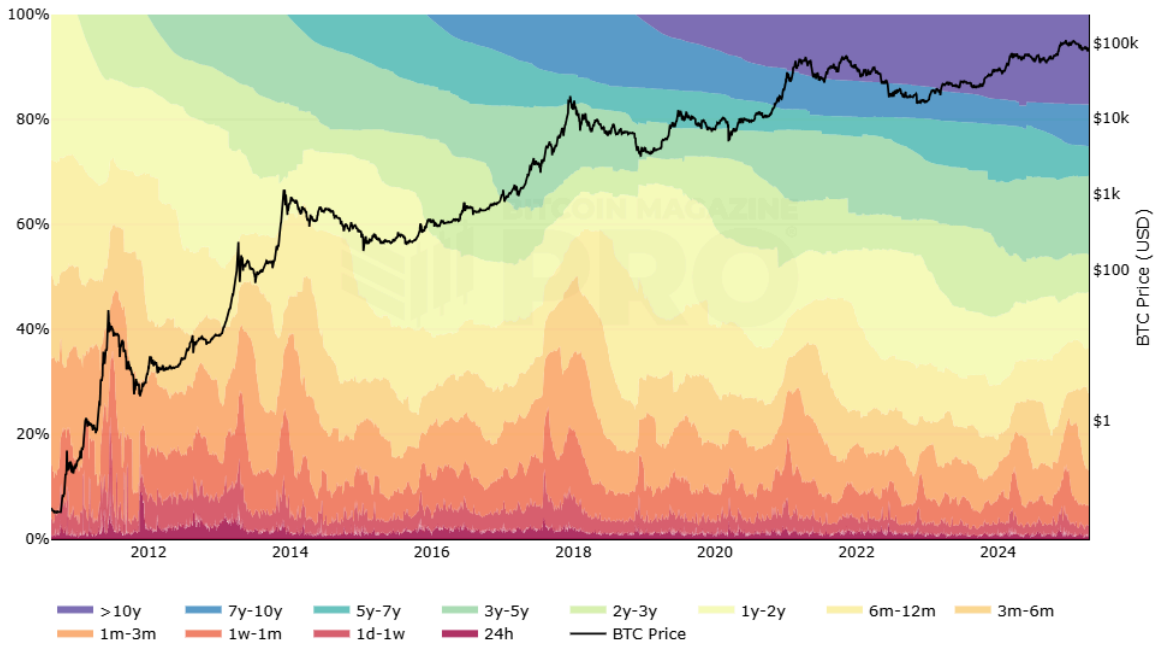
Fonte: Javier Pastor, 2023.

4.1.2 Transição para reserva de valor: Evidências

Diversos indicadores apontam para a efetivação da transição do Bitcoin de meio de troca para uma reserva de valor. Esses dados também evidenciam o crescimento da adoção do ativo, que passou a ser utilizado como estratégia primária de caixa por grandes empresas e como reserva estratégica por alguns governos. Neste tópico, serão apresentados gráficos e métricas que ilustram essa mudança de posicionamento em relação ao uso do Bitcoin.

Um dos comportamentos que reforçam a transição do Bitcoin para a função de reserva de valor é o crescimento contínuo da participação dos chamados *long-term holders* na rede. Já apresentado na fundamentação teórica, esse grupo representa usuários com perfil de retenção prolongada do ativo. A **Figura 18**, apresentada novamente nesta seção, agora é analisada sob o viés interpretativo dos resultados, revelando uma tendência consolidada: grande parte dos bitcoins em circulação permanece inativa por longos períodos, o que está alinhado com o comportamento esperado de um ativo utilizado como reserva de valor.

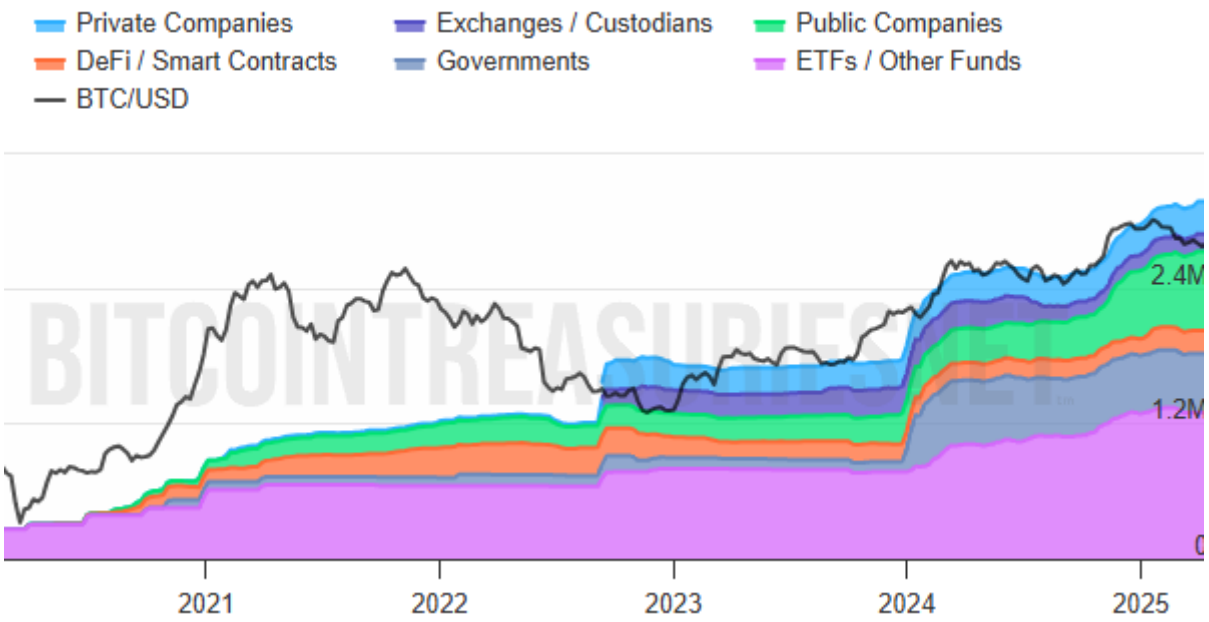
Figura 18: Análise do comportamento dos Long-Term Holders.



Fonte: BitcoinMagazine, 2025.

Esse comportamento de retenção por parte dos usuários não se limita apenas aos investidores individuais. Cada vez mais, instituições estão adotando uma postura semelhante, tratando o Bitcoin como um ativo estratégico de longo prazo. Outro dado que reforça essa tendência é apresentado pelo Bitcoin Treasuries, que evidencia o crescimento exponencial, nos últimos anos, do número de empresas públicas, privadas e até mesmo governos que vêm acumulando Bitcoin de forma contínua. Essa estratégia evidencia uma mudança no posicionamento institucional em relação ao ativo, como ilustrado na **Figura 19**.

Figura 19: Análise de retenção por governos e instituições.



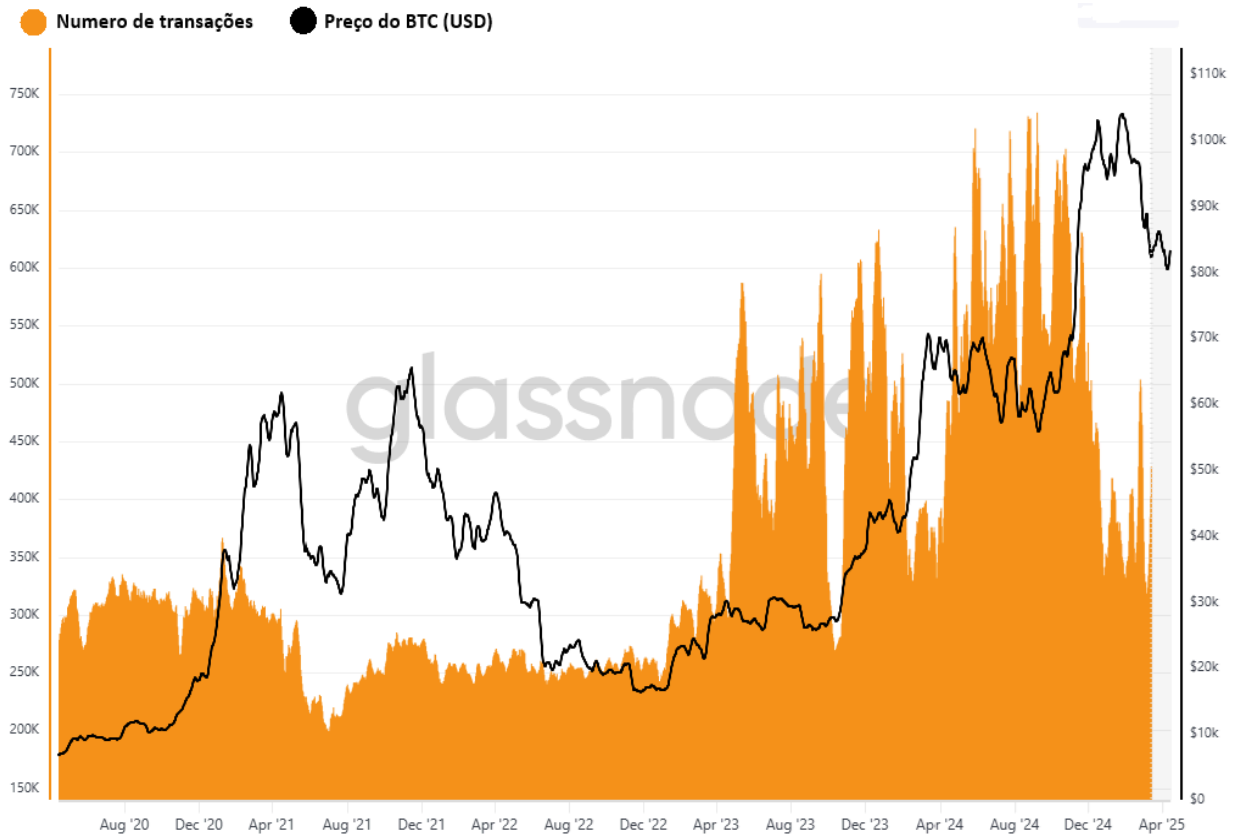
Fonte: BitcoinTreasures, 2025.

4.1.3 Novo propósito vs. Relevância da escalabilidade

Ao se consolidar como uma reserva de valor e não como um sistema para pagamentos do dia a dia, o Bitcoin passou a ser utilizado de forma menos frequente em transações cotidianas. Isso significa que o número de transações diárias tende a ser menor do que se a rede estivesse sendo usada por milhões de pessoas comprando produtos diariamente.

Essa mudança de foco pode ser percebida ao analisarmos a relação entre o número de transações na rede e o preço do ativo ao longo do tempo. A figura a seguir ilustra como, apesar da valorização expressiva do Bitcoin nos últimos anos, o volume diário de transações permaneceu relativamente estável. Esse comportamento reforça a ideia de que a rede tem sido utilizada predominantemente como reserva de valor, em vez de um meio de pagamento para uso cotidiano.

Figura 20: Volume de Transações vs Valor do Ativo.



Fonte: GlassNode, 2025.

Com base nos dados apresentados na **Figura 18**, observa-se que, nos últimos cinco anos, o valor de mercado do Bitcoin chegou a subir mais de 1500%. Em contrapartida, o volume de transações na rede, mesmo nos períodos de maior atividade, teve um crescimento máximo de cerca de 150%. Considerando o momento atual, a rede apresenta um volume de transações semelhante ao de cinco anos atrás, enquanto o ativo acumula uma valorização superior a 1000% no mesmo

intervalo. Esses dados evidenciam uma clara dissociação entre a demanda pelo ativo Bitcoin e a utilização da rede para transações.

Na prática, esse cenário reduz a urgência em resolver os desafios de escalabilidade da rede. Como consequência, soluções desenvolvidas com esse propósito, como as redes off-chain (por exemplo, a Lightning Network), acabam enfrentando menor demanda e adoção.

4.1.4 Micropagamentos vs Transações internacionais

O Bitcoin acabou não se consolidando como uma boa alternativa para micropagamentos, boa parte disso pode ser atribuída à questão da escalabilidade, que traz como consequências algumas características pouco atrativas.

A primeira é o tempo médio do intervalo entre a mineração de um bloco e o próximo, que leva cerca de 10 minutos, ou seja, uma transação pode levar até 10 minutos (ou um pouco mais), para ser efetivada.

A segunda é a taxa da rede, que como apontado na fundamentação deste trabalho, possui um custo médio que gira em torno de 10 a 30 sat/vByte, uma transação simples ocupa um espaço de aproximadamente 150 vBytes, ou seja, se no momento da transação o custo estiver em 20 sat/vByte e o valor de cotação do Bitcoin estiver em R$500.000,00 (Cotação atual em Abril de 2025) então teríamos a seguinte taxa:

20 (sat/vByte) * 150 (vBytes) = 3000 sats (Satoshis)

Satoshis são a menor medida do Bitcoin, 1 Satoshi corresponde a 0,00000001 BTC, então podemos concluir que 3000 Sats possui o valor de 0,00003000 BTC que na cotação do BTC em reais citado acima (R$500.000,00) teria o valor equivalente a R$15,00.

Com base nos pontos citados, sendo eles o tempo médio de mineração (10 minutos) e a taxa média estipulada no exercício acima (15 reais), podemos concluir que existem alternativas mais atrativas e eficientes para micropagamentos, como o

caso do Pix no Brasil, o qual não cobra taxas e as transações são realizadas de forma instantânea.

No entanto, é importante observar um contraponto interessante. Esperar 10 minutos e ter um custo de 15 reais não parece interessante para quem está tentando pagar por um sorvete em um shopping, mas e para quem quer transferir milhões para outro país ? Algo que é muito recorrente para grandes empresas e governos.

O custo por sat/vByte e o espaço ocupado em vBytes por uma transação não será alterado pelo valor transacionado, ou seja, se pagará a mesma taxa para enviar um valor em BTC equivalente a R$5,00 ou R$1.000.000,00.

De acordo com um estudo realizado por Sieradzan (2022), em 2020 a média de taxas cobradas por transações internacionais no valor de 200 dólares através de bancos foi de 7,27% enquanto o mesmo valor enviado via Bitcoin gerou uma taxa de 0,02%.

Os meios tradicionais para negociações internacionais possuem diversas taxas inclusas e *spread cambial*, negociações de grandes valores entre países possuem custos elevados e a transação leva dias para ser concluída por precisar passar por diferentes instituições. Em contrapartida, o Bitcoin nesse mesmo contexto, movimentando grandes valores entre países, leva os mesmos 10 minutos e custa a mesma taxa de uma pequena transação. Nesse exemplo notamos que traz uma grande economia, se mostrando uma alternativa interessante.

Portanto, apesar das limitações para transações cotidianas de baixo valor, o Bitcoin se destaca como uma ferramenta potente para transferências internacionais, especialmente em cenários onde eficiência, rapidez e neutralidade são cruciais.

4.2 Desafios Técnicos

Apesar de o Bitcoin ter evoluído de uma proposta de moeda digital para hoje ser mais vista como uma reserva de valor descentralizada, sua infraestrutura tecnológica ainda enfrenta desafios que limitam sua escalabilidade, usabilidade e adoção em larga escala.

4.2.1 Escalabilidade e Latência

Como já discutido anteriormente, a limitação no número de transações processadas por segundo é um dos entraves centrais da blockchain do Bitcoin. Este gargalo se deve ao tamanho fixo dos blocos e ao intervalo médio de 10 minutos por bloco, o que restringe a rede a cerca de 7 transações por segundo (TPS), em contraste com sistemas centralizados como a Visa, que processam milhares por segundo.

Essa limitação de escalabilidade impacta diretamente a experiência dos usuários e a viabilidade do uso massivo da rede. Durante períodos de alta demanda, o congestionamento do mempool — área onde ficam armazenadas as transações pendentes — causa elevação nas taxas de transação, uma vez que os usuários competem por espaço nos próximos blocos. Isso torna inviável o uso do Bitcoin em contextos que exigem operações rápidas e de baixo custo, como micropagamentos, transferências instantâneas ou serviços de alto volume.

Além disso, a latência — tempo necessário para que uma transação seja confirmada de forma segura — também se torna um fator limitante. Para muitas aplicações financeiras, especialmente aquelas que exigem liquidez imediata, a espera de 10 minutos por uma confirmação (ou mais, considerando múltiplas confirmações para maior segurança) pode ser considerada impraticável.

Esse cenário evidencia o desafio técnico enfrentado pela rede em equilibrar segurança, descentralização e escalabilidade — conhecido como o trilema da blockchain, um conceito amplamente discutido por Vitalik Buterin, fundador da

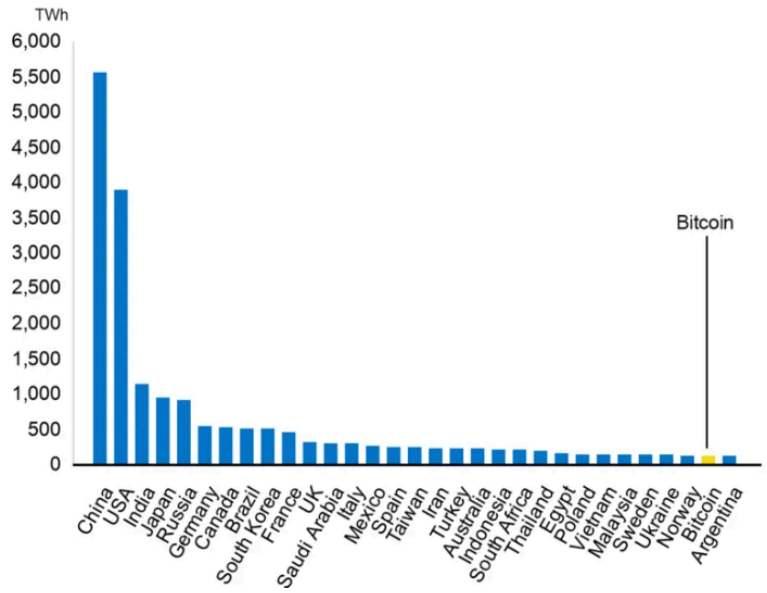
Ethereum. Soluções alternativas vêm sendo estudadas e propostas, como a adoção de redes complementares (redes de segunda camada) e melhorias na compactação e estrutura dos blocos. Contudo, tais abordagens nem sempre são consensuais ou fáceis de implementar, dada a estrutura descentralizada do protocolo.

4.2.2 Consumo energético do Proof of Work

O mecanismo de consenso baseado em Proof of Work, embora seguro e descentralizado, impõe um custo energético significativo. A necessidade de resolver puzzles criptográficos complexos exige muito poder computacional, que por sua vez consome grandes quantidades de eletricidade, levantando debates sobre a sustentabilidade da rede e questões ambientais.

O Cambridge Bitcoin Electricity Consumption Index estimou que, em 2021, o consumo anual de eletricidade da rede Bitcoin era de aproximadamente 121,36 terawatt-horas (TWh), superando o consumo de países inteiros como a Argentina. Segundo Cristina Criddle (2021), “se o Bitcoin fosse um país, ele estaria na trigésima posição no ranking dos que mais consomem energia elétrica.”

Figura 21: Ranking de consumo de energia elétrica.



Fonte: British Broadcasting Corporation (BBC), 2021.

Esse alto custo energético não apenas impacta o meio ambiente, como também levanta questionamentos sobre a viabilidade de longo prazo do modelo atual de consenso. Diante dessas preocupações, diversos projetos de blockchain vêm explorando soluções alternativas que mantenham a segurança e a descentralização, mas com menor impacto ambiental. Uma dessas alternativas é o Proof of Stake (PoS), um mecanismo que elimina a necessidade de mineração baseada em hardware e consequentemente o consumo de energia elétrica.

4.2.3 Tamanho da blockchain e armazenamento

Desde que a rede Bitcoin entrou em operação em janeiro de 2009, um novo bloco é adicionado aproximadamente a cada dez minutos, contendo um registro imutável de todas as transações validadas naquele intervalo. Isso significa que a blockchain é uma estrutura de dados em constante crescimento, já que cada novo bloco carrega um novo conjunto de informações e está criptograficamente vinculado ao bloco anterior, mantendo a integridade da cadeia desde o bloco gênese (bloco 0). Como consequência direta, o tamanho total da blockchain aumenta continuamente com o passar do tempo.

Esse crescimento acarreta desafios importantes relacionados ao armazenamento. Os chamados nós completos (full nodes), que mantêm uma cópia integral de toda a blockchain e participam ativamente da verificação de transações e blocos, precisam dispor de espaço em disco suficiente para armazenar esses dados. Além disso, devem ter capacidade computacional para processar e validar essas informações de forma eficiente.

À medida que o tamanho da blockchain aumenta, o requisito de armazenamento se torna uma barreira técnica para usuários comuns operarem nós completos em máquinas pessoais. Isso pode afetar diretamente a descentralização da rede, uma vez que menos participantes serão capazes de manter cópias completas da blockchain, aumentando a dependência de nós mantidos por grandes entidades ou organizações.

Além disso, há implicações na capacidade de auditoria independente. Um dos pilares da tecnologia blockchain é a possibilidade de qualquer pessoa, em teoria, poder verificar todas as transações de forma transparente. No entanto, se poucos usuários conseguirem operar nós completos devido ao tamanho da cadeia, essa transparência e auditabilidade podem ser comprometidas na prática.

4.2.4 Dificuldade de atualização e governança técnica

Realizar qualquer alteração no protocolo do Bitcoin como aumentar o tamanho do bloco ou implementar novas funcionalidades, demanda um extenso processo de coordenação e cooperação entre os diversos participantes da rede. Isso ocorre porque o Bitcoin não possui uma estrutura de governança centralizada, o que significa que decisões técnicas são tomadas de forma descentralizada, com base no consenso, assim como na validação dos blocos.

Essa ausência de um modelo de governança formal dificulta a adoção rápida de melhorias. Qualquer proposta de mudança precisa ser amplamente discutida, analisada, testada e, sobretudo, aceita por uma parte significativa dos nós e mineradores da rede. Essa dinâmica, embora contribua para a segurança e estabilidade do sistema, também torna o processo de atualização lento e sujeito a impasses.

Além disso, a necessidade de consenso entre os diferentes agentes da rede como desenvolvedores, mineradores, operadores de nós e usuários — pode gerar disputas que nem sempre resultam em soluções unificadas. Em alguns casos, a falta de acordo técnico e ideológico já levou a divisões na comunidade e à criação de redes alternativas com regras próprias.

Consequentemente, a dificuldade em realizar atualizações no protocolo representa um desafio técnico importante, pois limita a capacidade da rede de evoluir frente a novas demandas, ameaças ou oportunidades. Essa rigidez, embora proteja o sistema contra mudanças arbitrárias, pode comprometer sua capacidade de adaptação a longo prazo. Essas características rígidas e apolíticas (independente

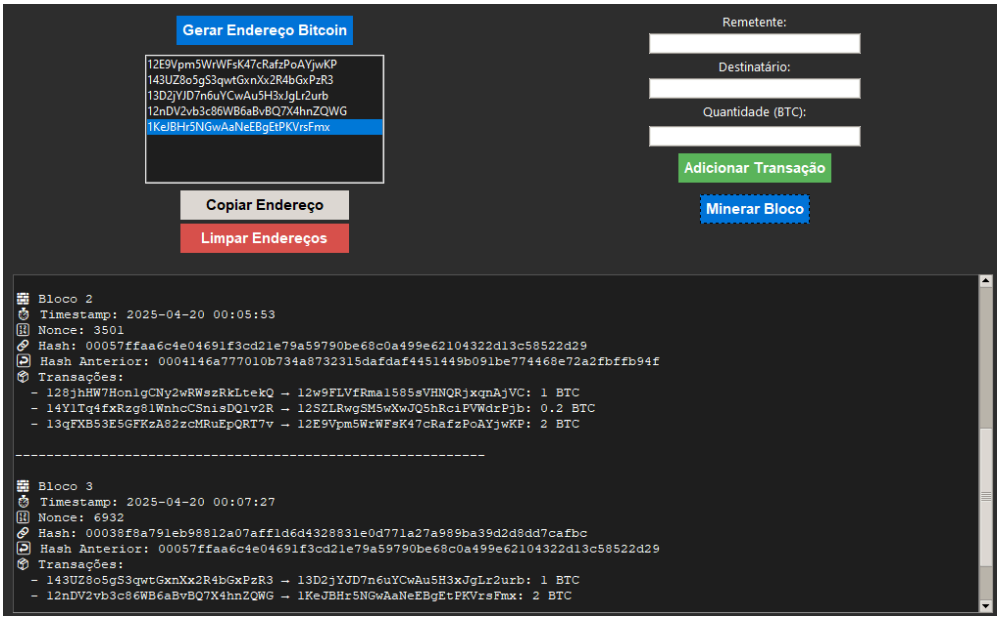
de governos) corroboram para a narrativa de que hoje o Bitcoin se tornou uma reserva de valor.

4.3 Simulador de Blockchain: Apresentação

Com o objetivo de reforçar os conceitos técnicos apresentados ao longo deste trabalho, foi desenvolvido um simulador de blockchain com interface gráfica, cujo foco principal é representar de forma visual e didática o funcionamento básico da tecnologia por trás do Bitcoin. Esse artefato técnico serve como um recurso complementar à fundamentação teórica, permitindo observar na prática os principais elementos que compõem uma rede blockchain.

O simulador foi projetado para abstrair os aspectos mais complexos da rede real, como comunicação peer-to-peer ou regras econômicas, e enfatizar os mecanismos fundamentais que sustentam a segurança e a estrutura do Bitcoin. Dessa forma, o usuário pode interagir com uma simulação simplificada que ilustra de maneira intuitiva conceitos como geração de chaves, criação de transações, mineração com prova de trabalho e encadeamento de blocos.

Figura 22: Interface do simulador.



Fonte: Autor, 2025.

A implementação foi realizada utilizando a linguagem de programação Python, com apoio da biblioteca gráfica Tkinter para construção da interface visual. Para a simulação dos mecanismos criptográficos, foram empregadas bibliotecas nativas como hashlib, responsável pela geração dos hashes SHA-256, e base58, utilizada na codificação dos endereços públicos.

O código-fonte completo do simulador está disponibilizado no **Apêndice B** deste trabalho, podendo ser utilizado livremente como ferramenta de apoio didático para estudantes, professores ou qualquer pessoa interessada em compreender os aspectos técnicos do funcionamento de uma blockchain. Sua criação está alinhada com a proposta metodológica deste estudo, que busca não apenas analisar teoricamente os desafios e mecanismos da blockchain, mas também proporcionar uma forma prática de explorá-los.

4.3.1 Funcionalidades do Simulador

O simulador desenvolvido apresenta funcionalidades que representam, de forma simplificada, os principais mecanismos da blockchain do Bitcoin. Cada funcionalidade foi implementada para aproximar o usuário dos conceitos técnicos fundamentais da rede.

Geração de endereços (chaves pública e privada): Permite a criação de pares de chaves criptográficas. A partir da chave pública, o endereço é gerado em base58, conforme o padrão do Bitcoin.

Criação de transações (*mempool*): Usuários simulam o envio de valores entre endereços gerados, com as transações sendo armazenadas temporariamente em um mempool.

Mineração com Proof of Work (PoW): Envolve validação das transações e resolução de um desafio computacional para encontrar um hash válido. A dificuldade é ajustável.

Visualização da cadeia de blocos: Os blocos minerados são encadeados visualmente, com dados como hash, nonce e transações, simulando a estrutura imutável da blockchain real.

Ainda que simplificadas, elas mantêm forte aderência aos princípios reais da tecnologia blockchain.

4.3.2 Limitações do Simulador

Apesar de representar de forma didática os principais mecanismos de funcionamento de uma blockchain como a do Bitcoin, o simulador desenvolvido possui algumas limitações que devem ser consideradas, especialmente no que se refere à sua aplicação prática e escopo técnico.

Ausência de verificação de saldo e validação de transações: O simulador permite a criação de transações entre endereços sem considerar o saldo disponível em cada um deles. Em uma blockchain real, cada transação passa por uma verificação rigorosa para garantir que os fundos utilizados realmente pertencem ao remetente e não foram gastos anteriormente (evitando o problema do double spending). No simulador, esse processo foi omitido para simplificar a experiência do usuário e manter o foco no aspecto estrutural da rede.

Inexistência de rede descentralizada (P2P): A blockchain do Bitcoin opera em um ambiente descentralizado com milhares de nós espalhados pelo mundo, que participam da validação de blocos, propagação de transações e manutenção da segurança da rede. No simulador, todos esses papéis são centralizados em uma única instância, o que não reflete a

complexidade e resiliência de uma rede peer-to-peer. Essa escolha foi feita com base em critérios didáticos e na limitação de recursos computacionais.

Limitações quanto à escalabilidade: O simulador não implementa mecanismos que permitam avaliar o desempenho da rede em cenários de alto volume transacional. Em uma blockchain real, como a do Bitcoin, a baixa escalabilidade é um dos principais desafios técnicos, limitando o número de transações por segundo (TPS) que podem ser processadas. Essa característica não é explorada no simulador, mas será discutida em detalhe no próximo tópico.

Segurança criptográfica simplificada: Embora o simulador utilize bibliotecas reais de criptografia (como hashlib e base58), a complexidade dos algoritmos utilizados na rede principal do Bitcoin — como ECDSA para assinaturas digitais e SHA-256 com duplo hashing — é representada de forma simplificada. O objetivo aqui é proporcionar uma visualização acessível do processo, sem demandar conhecimentos avançados em criptografia.

Essas limitações não comprometem a proposta do simulador, que é servir como ferramenta educacional. Pelo contrário, ajudam a reforçar a compreensão dos desafios enfrentados em uma blockchain real, ao contrastar a simplicidade do modelo com a complexidade do sistema em produção.

4.3.3 Relevância Técnica e Educacional do Simulador

O simulador de blockchain desenvolvido neste trabalho não se limita a uma representação visual dos conceitos discutidos, mas se estabelece como um artefato técnico com potencial de aplicação didática. Sua criação está alinhada com os objetivos da formação em Redes de Computadores, pois envolve conceitos de criptografia, estruturas de dados, redes distribuídas, interfaces gráficas e lógica de programação, promovendo uma integração prática entre teoria e tecnologia.

Do ponto de vista educacional, o simulador oferece a oportunidade para que estudantes, professores ou interessados possam interagir com os principais componentes da rede Bitcoin de forma intuitiva. Em vez de se limitarem a leituras ou descrições abstratas, os usuários podem observar e manipular elementos fundamentais como geração de endereços, criação de transações, validação via Proof of Work e visualização do encadeamento de blocos. Essa abordagem contribui para a assimilação de conceitos que muitas vezes são considerados complexos, especialmente por aqueles que estão tendo o primeiro contato com a tecnologia blockchain.

Nesse sentido, o artefato serve como ponte entre os aspectos conceituais e a aplicação técnica, reforçando o papel da prática no processo de aprendizagem. Sua inclusão neste trabalho é justificada não apenas como complemento à análise teórica da evolução da blockchain, mas também como uma contribuição efetiva à compreensão técnica e educacional dessa tecnologia por parte da comunidade acadêmica.

4.4 Simulador: Demonstração Prática

Com o objetivo de validar os conceitos técnicos abordados ao longo deste trabalho, o simulador foi utilizado em uma abordagem prática, explorando suas funcionalidades como recurso didático. Esta demonstração prática reforça a compreensão dos princípios da blockchain do Bitcoin a partir de uma perspectiva aplicada, conectando diretamente os conceitos à formação em Redes de Computadores.

Por meio da geração de endereços, criação e validação de transações, visualização do encadeamento dos blocos e simulação de mineração com Proof of Work, foi possível experimentar, de maneira interativa, os elementos que garantem segurança, integridade e descentralização em redes distribuídas, uma base fundamental da arquitetura do Bitcoin.

Ao simular o comportamento da rede, o estudante também se depara com conceitos-chave da área de redes, como comunicação ponto a ponto (P2P), redes distribuídas, certificados digitais, criptografia, algoritmos de hash e estruturas de dados. Isso demonstra a contribuição do simulador como ferramenta complementar de aprendizagem.

4.4.1 Cenários Simulados e Conceitos Técnicos Relacionados

A seguir, são apresentados alguns dos cenários testados:

1) Geração de Endereços Criptográficos: O simulador permite a geração de pares de chaves (pública e privada), aplicando os algoritmos de hash e codificação base58. Esse processo reforça a noção de segurança criptográfica, pilar essencial para autenticação e identificação dos usuários em redes blockchain.

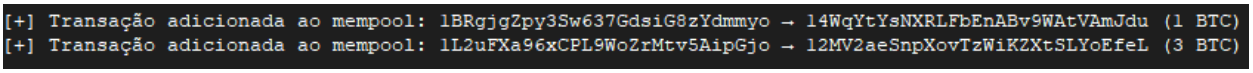
Figura 23: Geração de chaves e campos de entrada.

Fonte: Autor, 2025.

Conceito: segurança de redes e criptografia de chave pública.

2) Criação e Propagação de Transações: Transações simuladas são inseridas na mempool, aguardando inclusão em blocos. Essa etapa ilustra o comportamento de uma rede distribuída em que nós compartilham transações pendentes de validação.

Figura 24: Inserção de transação na mempool.

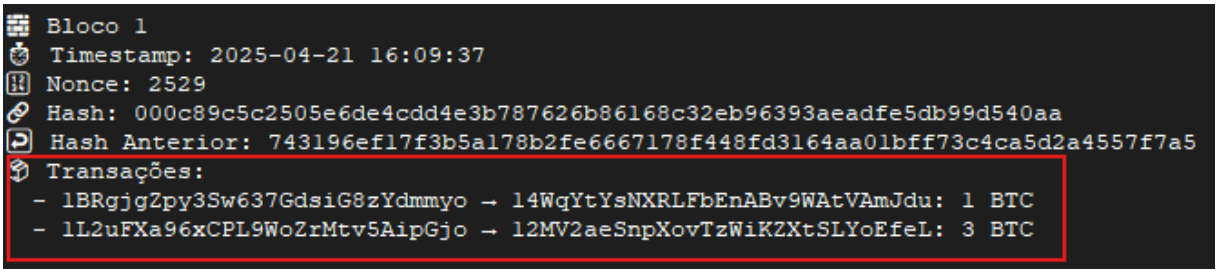


Fonte: Autor, 2025.

Conceito: redes ponto-a-ponto (P2P) e sincronização de dados.

3) Mineração e Prova de Trabalho (Proof of Work): Durante a mineração, o simulador realiza o cálculo do hash com base no conteúdo do bloco (cabeçalho + transações do mempool) e em um nonce variável até que o valor gerado satisfaça uma determinada dificuldade. Esse mecanismo ilustra a lógica de validação distribuída, onde os nós competem para propor blocos válidos.

Figura 25: Mineração de blocos.



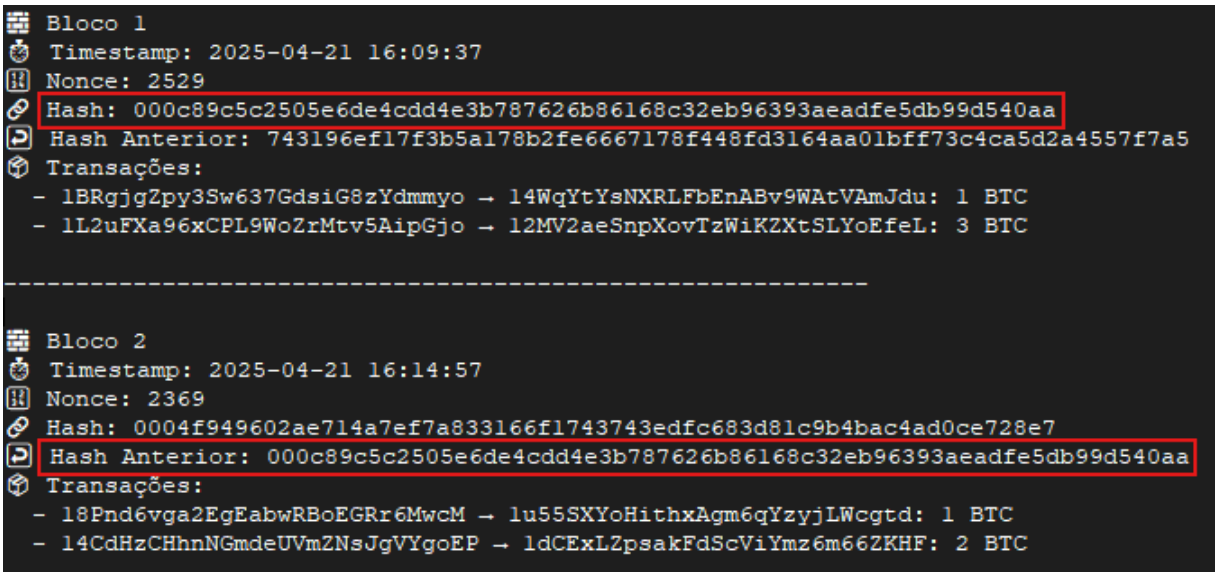
Fonte: Autor, 2025.

Conceito relacionado ao curso: processamento distribuído, integridade de dados e protocolos de consenso.

4) Encadeamento de Blocos: Ao criar blocos sucessivos, o simulador conecta cada bloco ao hash do anterior, formando uma cadeia imutável. Caso

algum dado seja alterado em um bloco anterior, os hashes subsequentes se tornam inválidos — representando a detecção de manipulação de dados.

Figura 26: Encadeamento dos blocos.



Fonte: Autor, 2025.

Conceito relacionado ao curso: controle de integridade em redes, rastreabilidade e verificação de consistência.

5) Verificação Visual da Imutabilidade: Embora o simulador não implemente diretamente um mecanismo automatizado de verificação da integridade da cadeia, como mostrado na **Figura 26** ele permite visualizar todos os hashes dos blocos, bem como os dados utilizados em sua construção. Isso possibilita ao usuário realizar, de forma manual ou conceitual, a análise da imutabilidade da cadeia.

Ao modificar um dado em um bloco anterior (por exemplo, o valor de uma transação), o hash do bloco é alterado, e essa mudança rompe a conexão com o bloco seguinte, cujo campo de “hash anterior” deixará de ser válido. Esse comportamento evidencia como a integridade da blockchain é mantida pelo encadeamento dos blocos via hashes criptográficos, e como qualquer alteração nos

dados compromete toda a sequência subsequente, reforçando o princípio da imutabilidade.

Essa visualização, mesmo sem validação automatizada, favorece o entendimento sobre a importância da integridade dos dados e como a arquitetura da blockchain detecta e desencoraja alterações maliciosas.

4.5 Considerações sobre o Artefato Desenvolvido

O simulador desenvolvido cumpre o papel de aproximar conceitos técnicos da blockchain a diversos tipos de públicos, reforçando o caráter exploratório e educativo da pesquisa. Ao aplicar conceitos fundamentais de encadeamento de blocos, hash criptográfico e validação de integridade, ele demonstra de forma prática os princípios que sustentam o funcionamento do Bitcoin e outras blockchains. Além disso, como ferramenta de TI, se alinha ao curso ao empregar lógica de programação, estrutura de dados e interface gráfica, sistemas distribuídos e algoritmos criptográficos, reforçando habilidades essenciais.

5 CONSIDERAÇÕES FINAIS

Este trabalho buscou analisar a evolução técnica da rede Bitcoin, destacando seus principais mecanismos, desafios estruturais e a mudança de propósito ao longo do tempo. A partir de uma revisão bibliográfica e documental, foi possível compreender como a proposta inicial de um sistema de dinheiro eletrônico ponto a ponto foi, gradualmente reinterpretada como uma reserva de valor, não apenas em razão de limitações operacionais, mas também por características que favorecem a proteção patrimonial, como a escassez do ativo, que oferece resistência à inflação, e a possibilidade de auto custódia, que garante ao usuário a posse integral de seus fundos, sem a necessidade de intermediários financeiros, muitas vezes suscetíveis a crises e problemas de solvência, especialmente em contextos de instabilidade econômica.

Foram apresentados os principais desafios enfrentados pela rede, como a baixa escalabilidade, o alto consumo energético do mecanismo de consenso Proof of Work, o crescimento contínuo do tamanho da blockchain e as dificuldades de atualização decorrentes da ausência de uma governança formal. Esses aspectos reforçam o caráter técnico da pesquisa e mostram como questões de infraestrutura impactam diretamente o uso da rede.

Como forma de consolidar os conceitos abordados, foi desenvolvido um simulador simplificado de blockchain, com foco nos principais elementos técnicos do Bitcoin: geração de endereços, criação de transações, mempool, mineração com prova de trabalho e visualização da cadeia de blocos. O simulador se propõe a ser uma ferramenta de apoio didático, permitindo ao usuário experimentar os processos fundamentais de uma rede blockchain de maneira interativa.

Além de apoiar a assimilação dos conceitos estudados, o simulador também representa a aplicação prática dos conhecimentos adquiridos ao longo do curso de Redes de Computadores, especialmente no que se refere às funções de hash, assinaturas digitais, rede ponto-a-ponto e sistemas distribuídos.

Conclui-se que o Bitcoin, apesar de suas limitações, representa um avanço significativo no campo das redes distribuídas e segurança da informação. O desenvolvimento do simulador cumpriu seu papel como artefato técnico, ampliando a compreensão dos mecanismos que sustentam essa tecnologia e oferecendo potencial uso educacional.

Para trabalhos futuros, sugere-se a expansão do simulador com novas funcionalidades, como a simulação de múltiplos nós, validação de blocos por consenso distribuído ou análise de cenários adversos, como ataques à rede, o que poderia contribuir ainda mais para o aprendizado técnico sobre sistemas blockchain.

REFERÊNCIAS BIBLIOGRÁFICAS

ALBRECHER, H.; FINGER, D.; GOFFARD, P. O. **Empirical risk analysis of mining a Proof-of-Work blockchain**. Decisions Econ Finan, 2024. Disponível em: https://link.springer.com/article/10.1007/s10203-024-00458-w#citeas. Acesso em: 09 abr. 2025.

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

BEVILACQUA, Luís Fernando; CORREIA, Luiz Gabriel; DA SILVA, Rafael Montoia. **Escalabilidade e possíveis soluções para redes blockchain**. 2018. Disponível em: https://www.researchgate.net/profile/Luiz-Correia/publication/367168268_Escalabilidade_e_possiveis_solucoes_para_redes_blockchain/links/63c532776fe15d6a5724dad5/Escalabilidade-e-possiveis-solucoes-para-redes-blockchain.pdf. Acesso em: 09 abr. 2025.

BITCOIN MAGAZINE PRO. **HODL Waves**. Disponível em: https://www.bitcoinmagazinepro.com/charts/hodl-waves. Acesso em: 15 abr. 2025.

BITCOIN TREASURIES. **Bitcoin Treasuries in Publicly Traded and Private Companies**. Disponível em: https://bitcointreasuries.net. Acesso em: 16 abr. 2025.

CALZA, Arthur de Souza et al. **A atividade dos mineradores de bitcoin frente os diferentes cenários: uma análise microeconômica**. 2023. Disponível em:https://repositorio.ufsc.br/bitstream/handle/123456789/252659/Monografia%20Arthur%20Calza.pdf?sequence=3&isAllowed=y. Acesso em: 11 abr. 2025.

CHEN, Tingfei. **Correlation Between Bitcoin Price and Total Supply of Long-term Holders**. Highlights in Business, Economics and Management, 2024. Disponível em:https://www.researchgate.net/publication/382587021_Correlation_Between_Bitcoin_Price_and_Total_Supply_of_Long-term_Holders. Acesso em: 17 abr. 2025.

CLAASSEN, Rutger. **Financial Crisis and the Ethics of Moral Hazard**. Social Theory and Practice, vol. 41, no. 3, 2015, pp. 527–51. JSTOR. Disponível em: http://www.jstor.org/stable/24575743. Acesso em: 09 nov. 2024.

CRIDDLE, Cristina. **Bitcoin consumes 'more electricity than Argentina**. BBC News, 10 fev. 2021. Disponível em: https://www.bbc.com/news/technology-56012952. Acesso em: 21 abr. 2025.

FIGUEIREDO, Daniel Duarte. **Fundamentos em blockchain**. Belo Horizonte: Instituto de Gestão e Tecnologia da Informação, 2020. Acesso em: 02 Nov. 2024.

GLASSNODE. **Bitcoin: Number of Transactions**. Disponível em: https://studio.glassnode.com/metrics?a=BTC&m=transactions.Count. Acesso em: 16 abr. 2025.

HASH FUNCTION. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2019. Disponível em: https://en.wikipedia.org/wiki/Hash_function. Acesso em: 15 out. 2024.

KREUTZ, Diego et al. **Introdução a Vulnerabilidades e Ataques em Blockchains e Criptomoedas**. 2024. Disponível em: https://www.researchgate.net/profile/Roben-Lunardi/publication/387861678_Introducao_a_Vulnerabilidades_e_Ataques_em_Blockchains_e_Criptomoedas/links/677fe474fb021f2a47e51277/Introducao-a-Vulnerabilidades-e-Ataques-em-Blockchains-e-Criptomoedas.pdf. Acesso em: 10 abr. 2025.

LAGO, Lucas. Blockchain: **confiança através de algoritmos**. Boletim, v. 2, n. 4, 2017. Disponível em: http://www.cest.poli.usp.br/wp-content/uploads/2018/08/V2N4-Blockchain-confian%C3%A7a-atrav%C3%A9s-de-algoritmos.pdf. Acesso em: 12 abr. 2025.

MACHADO, Victor. Experimento prático para integração da rede Bitcoin com a Rede Lightning. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/262217/TCC.pdf?sequence=1&isAllowed=y. Acesso em: 10 abr. 2025.

MENG, Xiaoqing; YUAN, Hong; CHEN, Jinyan. **The financial services industry and society: The role of incentives/punishments, moral hazard, and conflicts of interests in the 2008 financial crisis**. Journal of Economics, Finance and Administrative Science, [S.l.], v. 26, n. 52, p. 97–104, 2021. Disponível em: https://revistas.esan.edu.pe/index.php/jefas/article/view/120. Acesso em: 24 abr. 2025.

NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Whitepaper, 2008. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 12 abr. 2024.

NEELESH, Mungoli. **Deciphering the Blockchain: A Comprehensive Analysis of Bitcoin's Evolution, Adoption, and Future Implications**. 2013. Disponível em: https://www.researchgate.net/publication/369855143. Acesso em: 03 fev. 2025.

PEREIRA, Beno Matheus. **Dinâmica de sistemas aplicada à simulação de cenários na mineração de bitcoin**. 2025. Disponível em: https://repositorio.ufsm.br/bitstream/handle/1/34238/Pereira_Beno_Matheus_Saraiva_2025_TCC.pdf?sequence=1&isAllowed=y. Acesso em: 07 mar. 2025.

POON, Joseph; DRYJA, Thaddeus. **The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments**. Jan. 2016. Disponível em: https://lightning.network/lightning-network-paper.pdf. Acesso em: 01 abr. 2025.

REYNA, Ana; MARTÍN, Cristian; CHEN, Jaime; SOLER, Enrique; DIAZ, Manuel. **On blockchain and its integration with IoT**. Future Generation Computer Systems, v. 88, p. 173–190, nov. 2018. Disponível em: https://doi.org/10.1016/j.future.2018.05.046. Acesso em: 13 abr. 2025.

SIERADZAN, Paweł. **Cryptocurrencies as a means of payment: Bitcoin in relation to conventional currencies**. Zagreb International Review of Economics and Business, v. 25, n. 2, p. 69–85, 2022. Disponível em: https://doi.org/10.2478/zireb-2022-0025. Acesso em: 18 abr. 2025.

SWAN, M. **Blockchain: Blueprint for a New Economy**. O'Reilly Media, Inc., 2015.

TEMIN, Peter. **The Great Depression**. 1. ed. Cambridge: MIT Press, 1994. Disponível em: https://www.researchgate.net/publication/5182937_The_Great_Depression. Acesso em: 08 abr. 2025.

VIEIRA, Renato Melo; ARAÚJO, Wagner Junqueira de. **Assinatura de documentos eletrônicos utilizando certificados digitais: estudo de caso de assinaturas digitais aplicadas em atas de reuniões**. Revista Administração em Diálogo – RAD, Belo Horizonte, v. 20, n. 1, p. 1–15, 2021. Disponível em: https://periodicos.ufmg.br/index.php/moci/article/download/17435/14217/48574. Acesso em: 08 abr. 2025.

APÊNDICE

Apêndice A – Manual de Uso do Simulador de Blockchain

1. Visão Geral

O simulador de blockchain desenvolvido tem como objetivo ilustrar, de forma visual e interativa, os principais conceitos do funcionamento de uma blockchain baseada no modelo do Bitcoin. O sistema permite gerar endereços, criar e adicionar transações a um mempool, minerar blocos, e visualizar toda a cadeia de blocos resultante.

2. Requisitos

Para utilizar o simulador, é necessário ter o Python 3.6 ou superior instalado no sistema. O programa depende exclusivamente de bibliotecas da própria linguagem, exceto por uma, que deve ser instalada separadamente:

2.1 Bibliotecas utilizadas

tkinter - Biblioteca nativa para interfaces gráficas (GUI).

ttk - Submódulo do tkinter para widgets com estilo moderno.

hashlib - Utilizada para gerar os hashes dos blocos e chaves públicas.

threading - Utilizada para processar a mineração em segundo plano.

time - Utilizada para capturar o timestamp de cada bloco.

random - Geração aleatória de chaves privadas.

base58 - Codificação dos endereços Bitcoin.

2.2 Instalação de dependência externa

A única biblioteca externa necessária é base58, que pode ser instalada através de um prompt com o seguinte comando: pip install base58

Figura 27: Biblioteca base58.

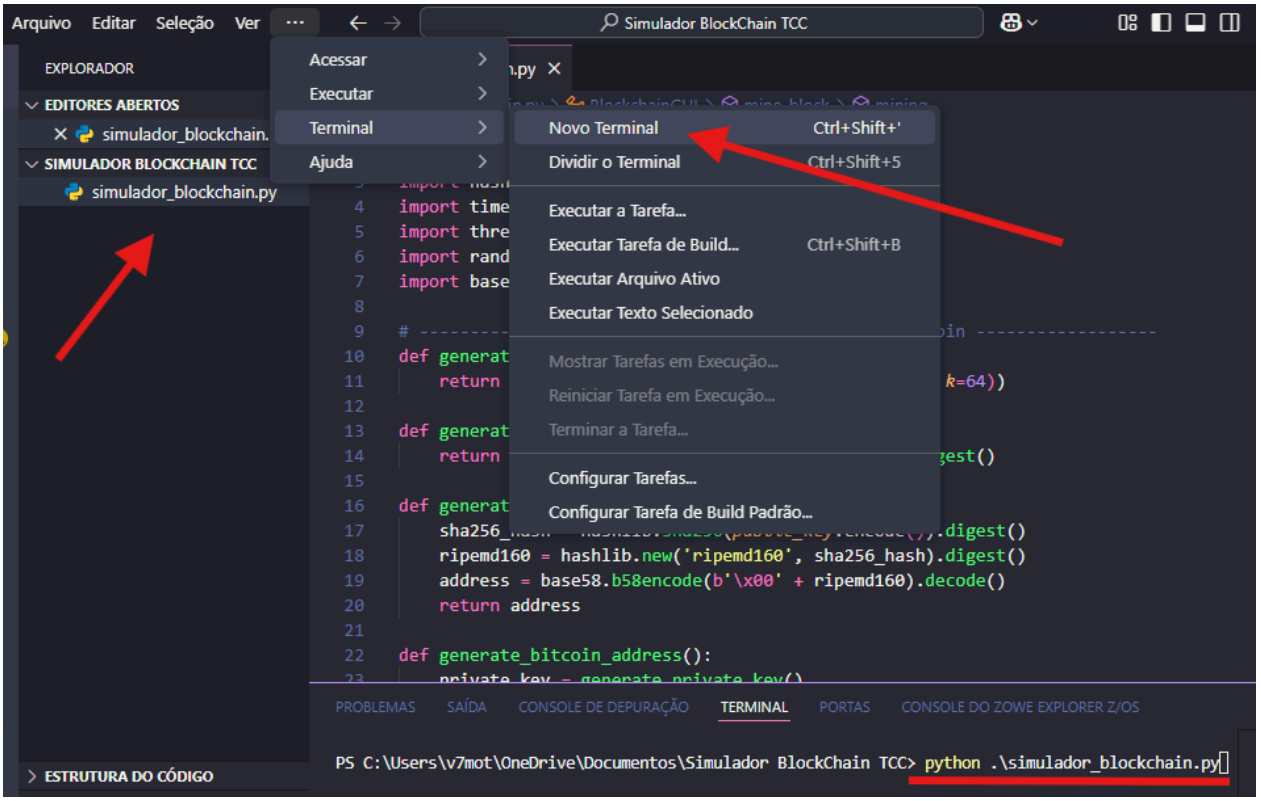
```
\Documentos\Simulador BlockChain TCC> pip install base58
```

Fonte: Autor, 2025.

3. Como Executar o Simulador

Após instalar o Python e a biblioteca base58, salve o código em um arquivo chamado simulador_blockchain.py e execute com: python simulador_blockchain.py

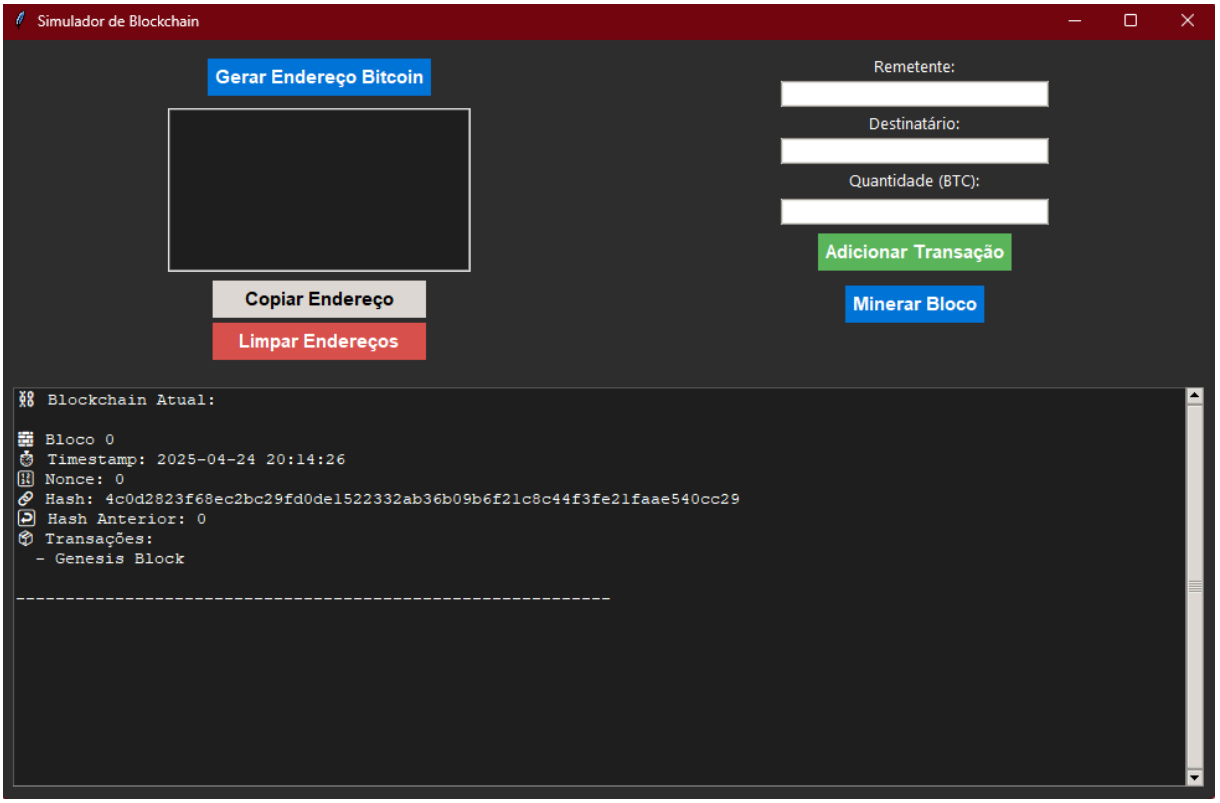
Figura 28: Execução da aplicação.



Fonte: Autor, 2025.

Uma janela gráfica será aberta com a interface do simulador.

Figura 29: Interface do simulador.



Fonte: Autor, 2025.

4. Funcionalidades da Interface

A interface é dividida em três seções principais:

4.1 Gerador de Endereços Bitcoin (lado esquerdo)

- Gerar Endereço Bitcoin: Cria um novo endereço utilizando funções de hash e codificação base58.

- Copiar Endereço: Copia o endereço selecionado para a área de transferência do sistema.

- Limpar Endereços: Remove todos os endereços listados.

4.2 Criação de Transações (lado direito)

- Remetente / Destinatário / Quantidade (BTC): Campos para preencher os dados de uma nova transação.

- Adicionar Transação: Adiciona a transação ao mempool e exibe a confirmação na área de saída inferior.

- Minerar Bloco: Inicia o processo de mineração de um novo bloco contendo todas as transações pendentes.

4.3 Área de Saída (inferior)

- Mostra a blockchain completa, bloco por bloco, com as seguintes informações:

- Índice do bloco

- Timestamp

- Hash do bloco atual e do anterior

- Lista de transações incluídas

5. Fluxo Básico de Uso

1. Gerar dois ou mais endereços Bitcoin.

Figura 30: Interface do simulador.

Fonte: Autor, 2025.

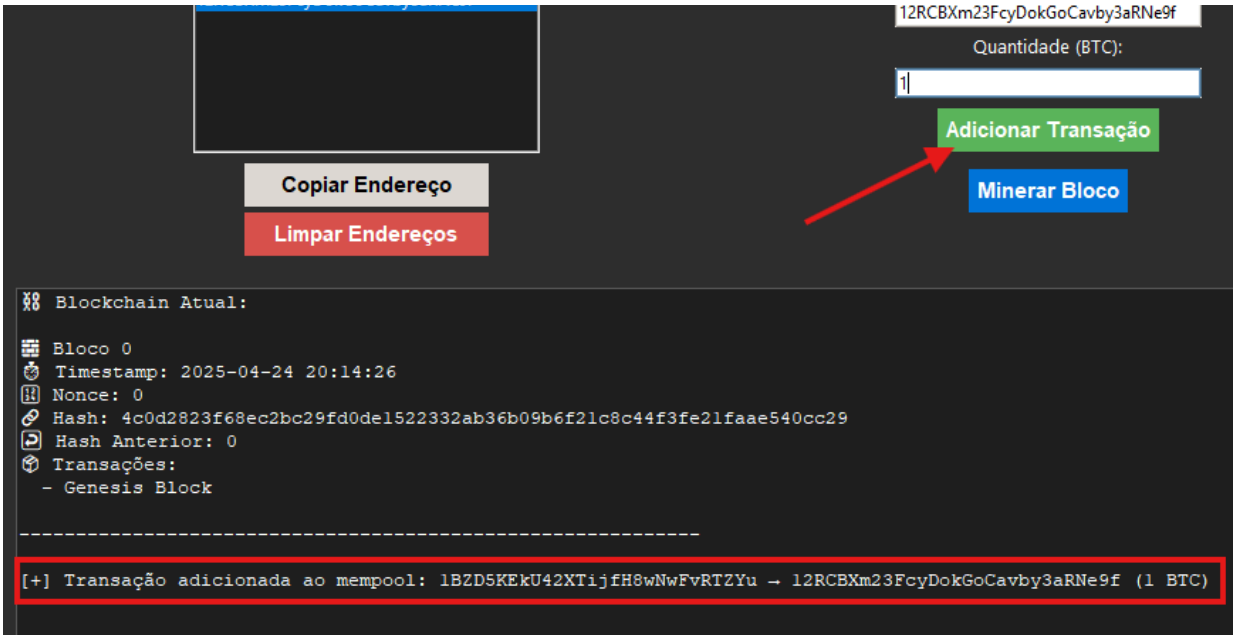
2. Criar uma transação preenchendo os campos de remetente e destinatário utilizando os endereços Bitcoin gerados e preencher o campo valor com a quantidade de BTC a ser enviado.

Figura 31: Preenchendo os campos.

Fonte: Autor, 2025.

3. Adicionar a transação ao mempool clicando no botão 'Adicionar Transação'.

Figura 32: Adicionando transação.



Fonte: Autor, 2025.

4. Repetir o passo anterior, se desejar, para incluir várias transações.

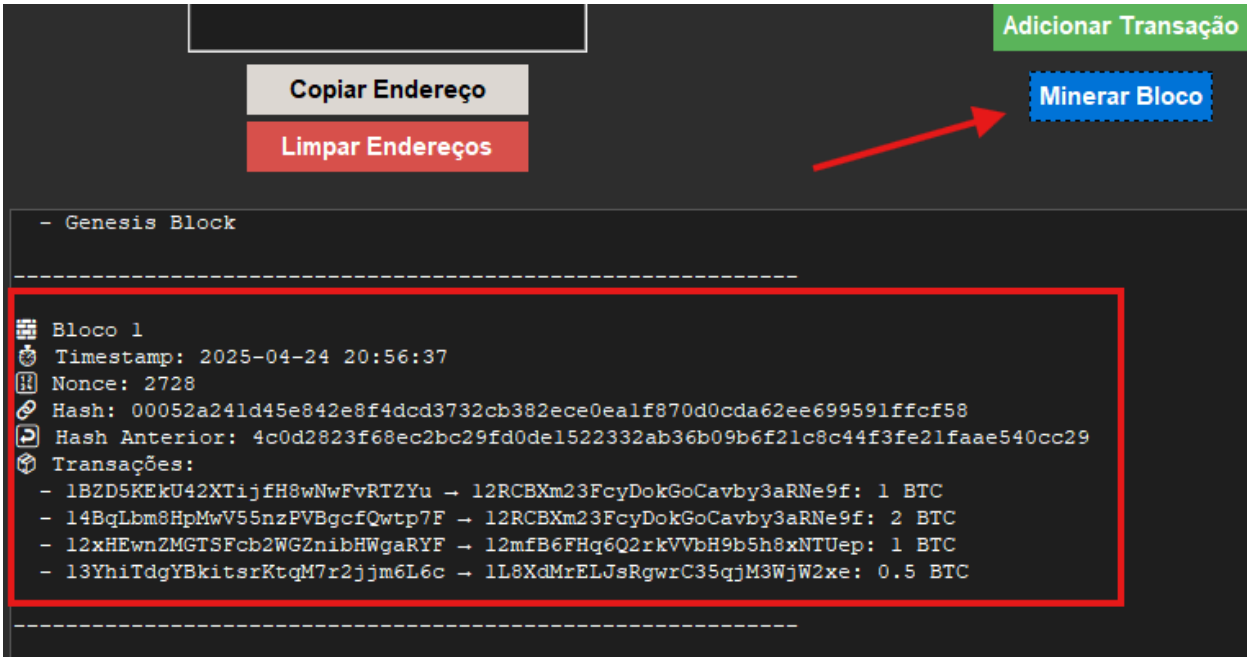
Figura 33: Transações no mempool.

```
[+] Transação adicionada ao mempool: 1BZD5KEkU42XTijfH8wNwFvRTZYu → 12RCBXm23FcyDokGoCavby3aRNe9f (1 BTC)
[+] Transação adicionada ao mempool: 14BqLbm8HpMwV55nzPVBgcfQwtp7F → 12RCBXm23FcyDokGoCavby3aRNe9f (2 BTC)
[+] Transação adicionada ao mempool: 12xHEwnZMGTSFcb2WGZnibHWgaRYF → 12mfB6FHq6Q2rkVVbH9b5h8xNTUep (1 BTC)
[+] Transação adicionada ao mempool: 13YhiTdgYBkitsrKtqM7r2jjm6L6c → 1L8XdMrELJsRgwrC35qjM3WjW2xe (0.5 BTC)
```

Fonte: Autor, 2025.

5. Minerar o bloco com as transações clicando em 'Minerar Bloco'.

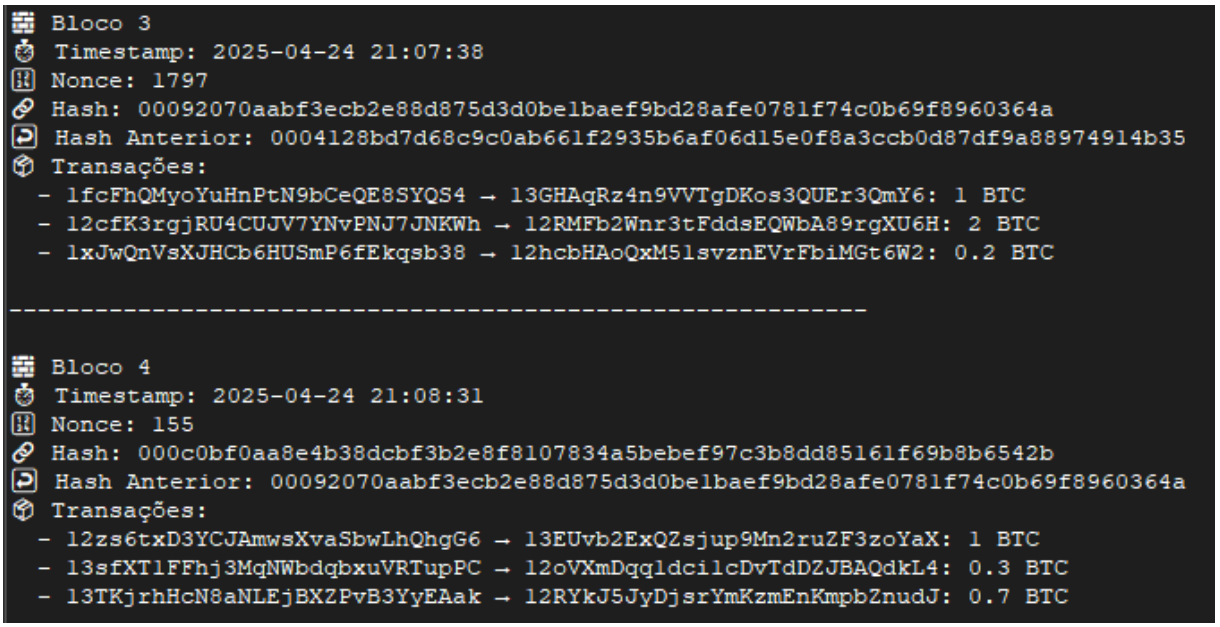
Figura 34: Mineração do bloco.



Fonte: Autor, 2025.

6. Acompanhar a atualização da blockchain na área inferior da interface.

Figura 35: Encadeamento dos blocos.



Fonte: Autor, 2025.

6. Considerações Técnicas

- O bloco gênesis é gerado automaticamente com a mensagem 'Genesis Block'.

- A dificuldade de mineração está fixada em 3, ou seja, os hashes precisam começar com três zeros (000...).

- Cada novo bloco é encadeado ao anterior, mantendo a integridade da cadeia.

- As transações são formatadas no estilo:

EndereçoRemetente → EndereçoDestinatário: X BTC

Apêndice B – Código-Fonte do Simulador de Blockchain

A seguir, apresenta-se o código-fonte completo da aplicação desenvolvida para este trabalho. O código foi escrito em linguagem Python e estruturado em um único arquivo denominado `simulador_blockchain.py`.

```
import tkinter as tk

from tkinter import ttk

import hashlib

import time

import threading

import random

import base58


# ---- Funções para gerar endereço Bitcoin ----#

def generate_private_key():

    return ''.join(random.choices('0123456789ABCDEF', k=64))


def generate_public_key(private_key):

    return hashlib.sha256(private_key.encode()).hexdigest()


def generate_address(public_key):

    sha256_hash = hashlib.sha256(public_key.encode()).digest()
```

```
    ripemd160 = hashlib.new('ripemd160', sha256_hash).digest()
    address = base58.b58encode(b'\x00' + ripemd160).decode()
    return address


def generate_bitcoin_address():
    private_key = generate_private_key()
    public_key = generate_public_key(private_key)
    return generate_address(public_key)


# ---- Estrutura do Bloco ----#
class Block:
    def __init__(self, index, previous_hash, transactions,
nonce=0):
        self.index = index
        self.timestamp = time.strftime("%Y-%m-%d %H:%M:%S")
        self.transactions = transactions
        self.previous_hash = previous_hash
        self.nonce = nonce
        self.hash = self.calculate_hash()


    def calculate_hash(self):
```

```
        block_string =
f"{self.index}{self.timestamp}{self.transactions}{self.previou
s_hash}{self.nonce}"

        return
hashlib.sha256(block_string.encode()).hexdigest()


    def mine_block(self, difficulty):

        target = '0' * difficulty

        while not self.hash.startswith(target):

            self.nonce += 1

            self.hash = self.calculate_hash()


# ---- Blockchain ----#

class Blockchain:

    def __init__(self):

        self.chain = [self.create_genesis_block()]

        self.difficulty = 3

        self.mempool = []


    def create_genesis_block(self):

        return Block(0, "0", ["Genesis Block"])
```

```
    def get_latest_block(self):
        return self.chain[-1]

    def add_transaction(self, sender, receiver, amount):
        transaction = f"{sender} → {receiver}: {amount} BTC"
        self.mempool.append(transaction)

    def mine_pending_transactions(self):
        if not self.mempool:
            return None
        new_block = Block(len(self.chain),
self.get_latest_block().hash, self.mempool[:])
        new_block.mine_block(self.difficulty)
        self.chain.append(new_block)
        self.mempool.clear()
        return new_block

# ---- Interface Gráfica ----#
class BlockchainGUI:
    def __init__(self, master):
        self.master = master
```

```
        master.title("Simulador de Blockchain")

        master.geometry("800x700")

        master.configure(bg="#2E2E2E")


        style = ttk.Style()

        style.theme_use("clam")

        style.configure("TButton", font=("Montserrat", 11,
"bold"), borderwidth=0, padding=5)

        style.configure("Add.TButton", background="#5CB85C",
foreground="white")

        style.configure("Mine.TButton", background="#0275D8",
foreground="white")

        style.configure("Gen.TButton", background="#D9534F",
foreground="white")

        style.configure("Clear.TButton", background="#D9534F",
foreground="white")


        self.blockchain = Blockchain()

        self.addresses = []


        top_frame = tk.Frame(master, bg="#2E2E2E")

        top_frame.pack(fill="both", expand=False, padx=10,
pady=10)
```

```
        left_frame = tk.Frame(top_frame, bg="#2E2E2E")

        left_frame.pack(side="left", fill="both", expand=True,
padx=5)


        right_frame = tk.Frame(top_frame, bg="#2E2E2E")

        right_frame.pack(side="right", fill="both",
expand=True, padx=5)


        self.generate_address_button = ttk.Button(left_frame,
text="Gerar Endereço Bitcoin", style="Gen.TButton",
command=self.generate_address)

        self.generate_address_button.pack(pady=5)


        self.address_listbox = tk.Listbox(left_frame,
height=8, width=40, bg="#1E1E1E", fg="white")

        self.address_listbox.pack(pady=5)


        self.copy_button = ttk.Button(left_frame, text="Copiar
Endereço", width=20, command=self.copy_address)

        self.copy_button.pack(pady=2)
```

```
        self.clear_button = ttk.Button(left_frame,
text="Limpar Endereços", width=20, style="Clear.TButton",
command=self.clear_addresses)

        self.clear_button.pack(pady=2)


        self.create_label(right_frame, "Remetente:")

        self.sender_entry = ttk.Entry(right_frame, width=35)

        self.sender_entry.pack(pady=2)


        self.create_label(right_frame, "Destinatário:")

        self.receiver_entry = ttk.Entry(right_frame, width=35)

        self.receiver_entry.pack(pady=2)


        self.create_label(right_frame, "Quantidade (BTC):")

        self.amount_entry = ttk.Entry(right_frame, width=35)

        self.amount_entry.pack(pady=5)


        self.add_button = ttk.Button(right_frame,
text="Adicionar Transação", style="Add.TButton",
command=self.add_transaction)

        self.add_button.pack(pady=2)
```

```
        self.mine_button = ttk.Button(right_frame,
text="Minerar Bloco", style="Mine.TButton",
command=self.mine_block)

        self.mine_button.pack(pady=10)


        self.output_frame = tk.Frame(master)

        self.output_frame.pack(pady=10, fill="both",
expand=True, padx=10)


        self.output = tk.Text(self.output_frame, height=15,
bg="#1E1E1E", fg="white", font=("Courier", 10))

        self.output.pack(side="left", fill="both",
expand=True)


        self.scrollbar = ttk.Scrollbar(self.output_frame,
command=self.output.yview)


self.output.configure(yscrollcommand=self.scrollbar.set)

        self.scrollbar.pack(side="right", fill="y")


        self.refresh_output()


    def create_label(self, frame, text):
```

```
        label = ttk.Label(frame, text=text,
foreground="white", background="#2E2E2E", font=("Segoe UI",
10))
        label.pack()


    def generate_address(self):
        new_address = generate_bitcoin_address()
        self.addresses.append(new_address)
        self.address_listbox.insert(tk.END, new_address)


    def copy_address(self):
        selected = self.address_listbox.curselection()
        if selected:
            address = self.address_listbox.get(selected[0])
            self.master.clipboard_clear()
            self.master.clipboard_append(address)
            self.master.update()


    def clear_addresses(self):
        self.address_listbox.delete(0, tk.END)


    def add_transaction(self):
```

```
        sender = self.sender_entry.get()
        receiver = self.receiver_entry.get()
        amount = self.amount_entry.get()
        if sender and receiver and amount:
            try:
                float(amount)
                self.blockchain.add_transaction(sender,
receiver, amount)
                transaction_msg = f"[+] Transação adicionada
ao mempool: {sender} → {receiver} ({amount} BTC)\n"
                self.output.insert(tk.END, transaction_msg)
                self.output.see(tk.END)
                self.sender_entry.delete(0, tk.END)
                self.receiver_entry.delete(0, tk.END)
                self.amount_entry.delete(0, tk.END)
            except ValueError:
                self.output.insert(tk.END, "[Erro] Quantidade
inválida!\n")

    def mine_block(self):
        def mining():
```

```
            new_block =
self.blockchain.mine_pending_transactions()

            self.refresh_output()

            if new_block:

                self.output.insert(tk.END, f"\n[✓] Bloco
{new_block.index} minerado com sucesso!\n")

        threading.Thread(target=mining).start()


    def refresh_output(self):

        self.output.delete(1.0, tk.END)

        self.output.insert(tk.END, "⛓ Blockchain Atual:\n\n")

        for block in self.blockchain.chain:

            self.output.insert(tk.END, f"🔷 Bloco
{block.index}\n")

            self.output.insert(tk.END, f"⏱ Timestamp:
{block.timestamp}\n")

            self.output.insert(tk.END, f"🔢 Nonce:
{block.nonce}\n")

            self.output.insert(tk.END, f"🔑 Hash:
{block.hash}\n")

            self.output.insert(tk.END, f"↩ Hash Anterior:
{block.previous_hash}\n")

            self.output.insert(tk.END, "📦 Transações:\n")

            for tx in block.transactions:
```

```
                self.output.insert(tk.END, f"  - {tx}\n")
            self.output.insert(tk.END, "\n" + "-"*60 + "\n\n")


# ---- Execução ----#
if __name__ == "__main__":
    root = tk.Tk()
    app = BlockchainGUI(root)
    root.mainloop()
```