PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CRIPTOMOEDAS E BLOCKCHAIN: UMA ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM

SERGIO JOSE DE ALMEIDA FILHO

GOIÂNIA
2026

SERGIO JOSE DE ALMEIDA FILHO

CRIPTOMOEDAS E BLOCKCHAIN: UMA ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Ciência da Computação.
Orientador(a): Prof. Me. Eugênio Júlio Messala Cândido Carvalho
Banca examinadora:

Prof. Me. Daniel Correa da Silva
Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA
2026

SERGIO JOSE DE ALMEIDA FILHO

CRIPTOMOEDAS E BLOCKCHAIN: UMA ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Ciência da Computação, em _____/_____/_____.

_____
Orientador(a): Prof. Me. Eugênio Júlio Messala Cândido Carvalho

_____
Membro 1: Prof. Me. Daniel Correa da Silva

_____
Membro 2: Prof. Me. Gustavo Siqueira Vinhal

GOIÂNIA
2026

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, pela força, sabedoria e oportunidade de chegar até esta etapa tão importante da minha trajetória.

À minha mãe, Andréia Rodrigues Moraes, bem como à minha família, expresso minha profunda gratidão pelo apoio, incentivo, paciência e confiança ao longo de toda essa caminhada. Foram essenciais nos momentos de dificuldade e fundamentais para que eu pudesse seguir em frente com dedicação e perseverança.

À minha namorada, Izabel Bonifácio Noleto, que tem caminhado ao meu lado há mais de seis anos, meu muito obrigado por ser meu porto seguro. Seu amor, paciência e companheirismo inabalável foram essenciais para que eu mantivesse o foco e a tranquilidade, não apenas na elaboração deste trabalho, mas durante toda a minha jornada acadêmica.

Aos meus professores, agradeço pelos ensinamentos, orientações e conhecimentos compartilhados durante o curso. Cada contribuição foi importante para a minha formação acadêmica, profissional e pessoal.

A todos que, de alguma forma, contribuíram para a realização deste trabalho, deixo meu sincero agradecimento.

RESUMO

A digitalização crescente da economia transformou profundamente a forma como o dinheiro é registrado, transferido e controlado. Atualmente, os recursos financeiros existem majoritariamente como registros em sistemas computacionais, cuja validade e circulação dependem de intermediários centralizados, como bancos e instituições financeiras, responsáveis por garantir a confiança entre as partes. Foi nesse cenário que o surgimento do Bitcoin, em 2008, e, posteriormente, do Ethereum introduziu a tecnologia *blockchain* como alternativa descentralizada para registrar e transferir valor, sem a necessidade de uma autoridade central. Embora frequentemente mencionadas em conjunto, essas duas redes foram concebidas com propósitos e arquiteturas distintos, e suas diferenças nem sempre são compreendidas com clareza. Diante disso, este trabalho analisa comparativamente as arquiteturas do Bitcoin e do Ethereum, com o objetivo de identificar suas principais convergências, diferenças estruturais e implicações práticas no contexto da tecnologia *blockchain*. Para isso, são apresentados os fundamentos técnicos que sustentam as criptomoedas e as redes *blockchain* — como estrutura de blocos, funções *hash*, rede *peer-to-peer*, mecanismos de consenso, mineração, chaves criptográficas, transações, privacidade e contratos inteligentes —, seguidos da análise individual de cada rede e de uma comparação sistemática entre elas, com base em critérios como filosofia de *design*, modelo transacional, mecanismo de consenso, escalabilidade, privacidade, auditabilidade e aplicações. Os resultados indicam que Bitcoin e Ethereum compartilham fundamentos comuns da *blockchain*, mas foram desenvolvidos para finalidades distintas: o Bitcoin se destaca como sistema descentralizado de transferência e preservação de valor, enquanto o Ethereum se consolida como infraestrutura programável para contratos inteligentes e aplicações descentralizadas.

Palavras-chave: Blockchain. Criptomoedas. Bitcoin. Ethereum. Contratos inteligentes.

ABSTRACT

The growing digitalization of the economy has profoundly transformed the way money is recorded, transferred, and controlled. Today, financial resources exist mostly as records in computational systems, whose validity and circulation depend on centralized intermediaries, such as banks and financial institutions, responsible for ensuring trust between the parties. It was in this context that the emergence of Bitcoin, in 2008, and later of Ethereum, introduced blockchain technology as a decentralized alternative for recording and transferring value, without the need for a central authority. Although they are often mentioned together, these two networks were designed with distinct purposes and architectures, and their differences are not always clearly understood. In light of this, this work comparatively analyzes the architectures of Bitcoin and Ethereum, aiming to identify their main convergences, structural differences, and practical implications in the context of blockchain technology. To this end, it presents the technical foundations that support cryptocurrencies and blockchain networks — such as block structure, hash functions, peer-to-peer networks, consensus mechanisms, mining, cryptographic keys, transactions, privacy, and smart contracts — followed by an individual analysis of each network and a systematic comparison between them, based on criteria such as design philosophy, transaction model, consensus mechanism, scalability, privacy, auditability, and applications. The results indicate that Bitcoin and Ethereum share common blockchain foundations but were developed for different purposes: Bitcoin stands out as a decentralized system for value transfer and preservation, whereas Ethereum has established itself as a programmable infrastructure for smart contracts and decentralized applications.

Keywords: Blockchain. Cryptocurrencies. Bitcoin. Ethereum. Smart contracts.

LISTA DE ILUSTRAÇÕES

Figura 1 – Fluxograma simplificado mostrando os 6 passos de uma transação na blockchain. 20
Figura 2 – Representação dos blocos em um blockchain. 21
Figura 3 – Bifurcação na cadeia de blocos. 30
Figura 4 – Inclusão de uma transação em um bloco da blockchain. 34
Figura 5 – Estrutura de um bloco do blockchain do sistema Bitcoin. 35
Figura 6 – Representação de uma Árvore de Merkle. 36
Figura 7 – Blocos conectados em uma cadeia, cada um referenciando o hash do cabeçalho do bloco anterior. 38
Figura 8 – Exemplo do mecanismo de nonce no protocolo de prova de trabalho. ... 43
Figura 9 – Curva de fornecimento controlado do Bitcoin e impacto dos eventos de halving. 45
Figura 10 – Representação da função de transição de estado no Ethereum. 53
Figura 11 – Contas e seus estados no Ethereum. 54
Figura 12 – Arquitetura e contexto de execução da Ethereum Virtual Machine. 57
Figura 13 – Web3: estrutura de uma web descentralizada baseada em contratos inteligentes e tecnologias P2P. 64

LISTA DE QUADROS

Quadro 1 – Síntese comparativa entre Bitcoin e Ethereum 76

LISTA DE SIGLAS

DApps	Decentralized Applications
ECDSA	Elliptic Curve Digital Signature Algorithm
EIP-1559	Ethereum Improvement Proposal 1559
EIP-4844	Ethereum Improvement Proposal 4844
EVM	Ethereum Virtual Machine
IP	Internet Protocol
P2P	Peer-to-Peer
PoS	Proof-of-Stake
PoW	Proof-of-Work
RIPEMD-160	RACE Integrity Primitives Evaluation Message Digest 160-bit
SHA-256	Secure Hash Algorithm 256-bit
STXO	Spent Transaction Output
UTXO	Unspent Transaction Output

SUMÁRIO

1 INTRODUÇÃO 12
1.1 Contextualização do tema 12
1.2 Motivação e justificativa 13
1.3 Relevância da pesquisa 13
1.4 Breve histórico e principais obras 14
1.5 Vantagens e diferencial em relação a trabalhos anteriores 15
1.6 Objetivos 15
1.6.1 Objetivo Geral 16
1.6.2 Objetivos específicos 16
1.7 Metodologia e organização do trabalho 16

2 FUNDAMENTOS DA BLOCKCHAIN E DAS CRIPTOMOEDAS 18
2.1 Conceito de blockchain 19
2.2 Estrutura de blocos e encadeamento 20
2.3 Funções hash criptográficas e integridade dos dados 22
2.4 Rede P2P e validação distribuída 23
2.5 Mecanismos de consenso e Prova de Trabalho 24
2.6 Mineração, criação de blocos e incentivos econômicos 25
2.7 Chaves criptográficas, endereços e carteiras 26
2.8 O ciclo de vida de uma transação 27
2.9 Transparência, privacidade e bifurcações 28
2.10 Aplicações da blockchain além das criptomoedas 30

3 A ARQUITETURA DO BITCOIN 32
3.1 O surgimento do Bitcoin e o problema do gasto duplo 32
3.2 A estrutura dos blocos, do blockchain e da rede P2P 34
3.3 O modelo de transações baseado em UTXOs 39
3.4 Mineração e consenso por Prova de Trabalho 41
3.5 A política monetária do Bitcoin e o halving 44
3.6 Escalabilidade no Bitcoin e a Lightning Network 45
3.7 Pseudonimato e rastreabilidade no Bitcoin 46
3.8 Síntese do capítulo 48

4 A ARQUITETURA DO ETHEREUM 50
4.1 O surgimento do Ethereum e a expansão da proposta da blockchain 50
4.2 Blocos, transações e estado global da rede Ethereum 52
4.3 O modelo de contas no Ethereum 53
4.4 Ethereum Virtual Machine (EVM) e contratos inteligentes 55
4.5 Gas, taxas e custo computacional 58
4.6 A transição do Ethereum da Proof-of-Work para a Proof-of-Stake 60

4.7 Escalabilidade no Ethereum 61
4.8 Transparência, privacidade e aplicações do Ethereum 62
4.9 Síntese do capítulo 65

5 ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM 67
5.1 Critérios e objetivos da análise comparativa..... 67
5.2 Filosofia de design e arquitetura de rede..... 68
5.3 Gestão de estado nos modelos UTXO e de contas..... 69
5.4 Consenso e segurança no Proof-of-Work e no Proof-of-Stake..... 71
5.5 Escalabilidade e soluções de segunda camada 72
5.6 Privacidade, auditabilidade e espectro de aplicações 74
5.7 Síntese dos resultados comparativos 75

6 CONCLUSÃO 78

REFERÊNCIAS.....80

1 INTRODUÇÃO

O avanço das criptomoedas e da tecnologia *blockchain* tem ampliado o interesse acadêmico e técnico por sistemas descentralizados de registro, validação e transferência de valor. Nesse contexto, Bitcoin e Ethereum destacam-se como duas das principais redes do ecossistema *blockchain*, embora tenham sido desenvolvidas com finalidades e arquiteturas distintas. Assim, esta introdução apresenta o contexto do tema, a motivação e a relevância da pesquisa, o panorama das principais obras relacionadas, os objetivos do trabalho e a forma como o estudo está organizado.

1.1 Contextualização do tema

A evolução do dinheiro acompanha as transformações econômicas e sociais da humanidade. Ao longo do tempo, diferentes formas de representação de valor foram utilizadas, desde bens físicos e metais preciosos até sistemas monetários centralizados operados por Estados e instituições financeiras. Com a digitalização crescente da economia, o dinheiro passou a existir majoritariamente como registros em sistemas computacionais, cuja validade e circulação dependem da confiança em intermediários responsáveis pelo controle, validação e armazenamento dessas informações (ALVES, 2022).

Nesse contexto, o surgimento do Bitcoin, em 2008, representou uma mudança importante na forma de pensar transferências digitais de valor. Pela primeira vez, foi proposta uma arquitetura capaz de realizar transações ponto a ponto sem a necessidade de uma autoridade central, utilizando criptografia, rede distribuída e mecanismos de consenso para garantir a integridade do sistema (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019). A relevância dessa proposta pode ser observada no crescimento alcançado pelo Bitcoin no ecossistema financeiro digital. Em julho de 2024, sua capitalização de mercado era estimada em aproximadamente US$ 1,1 trilhão, evidenciando a dimensão econômica alcançada por esse ativo no debate sobre sistemas monetários descentralizados (SEMLER SCIENTIFIC, 2024).

Com o passar do tempo, esse horizonte foi ampliado pelo Ethereum, que estendeu a proposta da *blockchain* ao incorporar uma arquitetura programável voltada à execução de contratos inteligentes e aplicações descentralizadas. Dessa forma,

Bitcoin e Ethereum consolidaram-se como duas das principais referências do ecossistema *blockchain*, embora com finalidades, estruturas e capacidades distintas (BUTERIN, 2014; FIGUEIREDO; LIMA, 2021).

1.2 Motivação e justificativa

A escolha do tema deste trabalho decorre da relevância crescente das criptomoedas e da tecnologia *blockchain* no cenário contemporâneo. Essas tecnologias passaram a influenciar debates sobre sistemas de pagamento, descentralização, segurança digital, automação de processos e novos modelos de interação econômica e computacional. Assim, compreender como essas redes são estruturadas e quais problemas procuram resolver tornou-se uma questão importante tanto do ponto de vista técnico quanto acadêmico.

Além disso, embora Bitcoin e Ethereum sejam frequentemente mencionados em conjunto, nem sempre suas diferenças são apresentadas de forma clara e sistemática. Em muitos casos, a discussão pública sobre essas redes se concentra em aspectos de mercado, valorização ou popularidade, deixando em segundo plano os elementos arquiteturais que explicam seus propósitos distintos. Por isso, justifica-se a realização de um estudo que compare essas duas plataformas a partir de seus fundamentos técnicos, destacando como diferentes escolhas de projeto impactam segurança, programabilidade, escalabilidade, privacidade e espectro de aplicações.

No âmbito da Ciência da Computação, especificamente, a compreensão dessas arquiteturas é relevante para profissionais que desenvolvem, integram ou avaliam sistemas baseados em *blockchain*. Conceitos como estruturas de dados distribuídas, algoritmos de consenso, criptografia aplicada e execução de código em ambientes descentralizados estão diretamente relacionados a competências técnicas da área, o que reforça a pertinência acadêmica desta pesquisa.

1.3 Relevância da pesquisa

A relevância desta pesquisa pode ser observada em três dimensões complementares. Em primeiro lugar, há uma relevância acadêmica, pois o trabalho organiza e sistematiza conceitos centrais da tecnologia *blockchain* a partir de um recorte comparativo entre duas redes de grande importância no campo das

criptomoedas. Em segundo lugar, há relevância técnica, uma vez que a análise das arquiteturas do Bitcoin e do Ethereum contribui para a compreensão de mecanismos como consenso distribuído, gestão de estado, execução programável e soluções de escalabilidade. Por fim, existe relevância prática, pois o estudo oferece uma base conceitual útil para estudantes, pesquisadores e profissionais interessados em tecnologias descentralizadas.

Ao desenvolver uma comparação entre Bitcoin e Ethereum com base em critérios técnicos, esta pesquisa contribui para superar visões simplificadas que tratam essas redes como equivalentes. Em vez disso, procura demonstrar que ambas se apoiam em fundamentos comuns da *blockchain*, mas respondem a objetivos diferentes e apresentam implicações práticas distintas.

1.4 Breve histórico e principais obras

A formulação moderna das criptomoedas e da *blockchain* tem como marco principal o artigo *Bitcoin: A Peer-to-Peer Electronic Cash System*, publicado por Satoshi Nakamoto em 2008. Nesse trabalho, foi proposta uma arquitetura descentralizada capaz de resolver o problema do gasto duplo sem a necessidade de uma autoridade central, estabelecendo as bases para o desenvolvimento de sistemas monetários digitais distribuídos (NAKAMOTO, 2008).

Posteriormente, diferentes autores passaram a aprofundar os fundamentos e as implicações da *blockchain*. Chervinski e Kreutz (2019), por exemplo, discutem elementos estruturais como blocos, funções *hash*, consenso e rede P2P, contribuindo para a compreensão da base técnica dessas redes. Alves (2022) apresenta uma discussão sobre a evolução do dinheiro e o contexto que favoreceu o surgimento das criptomoedas. Figueiredo e Lima (2021) exploram o avanço da *blockchain* para além das criptomoedas, especialmente no campo dos contratos inteligentes.

No contexto do Ethereum, Vitalik Buterin (2014) apresentou a proposta de uma *blockchain* programável, capaz de sustentar contratos inteligentes e aplicações descentralizadas. Essa arquitetura foi formalizada tecnicamente por Gavin Wood no *Yellow Paper* e aprofundada de forma didática por Antonopoulos e Wood (2018), que explicam o funcionamento da *Ethereum Virtual Machine*, do modelo de contas e do ecossistema de aplicações da rede (BUTERIN, 2014; WOOD, 2025; ANTONOPOULOS; WOOD, 2018). No que diz respeito à comparação entre as duas

plataformas, Lucena e Henriques (2016) desenvolveram um estudo sobre as arquiteturas do Bitcoin e do Ethereum, analisando suas principais estruturas técnicas. Já Antonopoulos e Harding (2023) oferecem uma visão atualizada e aprofundada do Bitcoin, abordando tanto seus fundamentos quanto seus desenvolvimentos mais recentes, como a *Lightning Network.*

1.5 Vantagens e diferencial em relação a trabalhos anteriores

O diferencial deste trabalho em relação a estudos anteriores sobre *blockchain* e criptomoedas está na ênfase comparativa entre Bitcoin e Ethereum, orientada por critérios arquiteturais e funcionais sistemáticos. Lucena e Henriques (2016), por exemplo, desenvolveram uma comparação entre as duas redes, porém com escopo mais restrito e sem incorporar desenvolvimentos mais recentes, como a transição do Ethereum para *Proof-of-Stake*, as soluções de escalabilidade de segunda camada e o protocolo EIP-4844. Este trabalho busca, portanto, oferecer uma análise mais abrangente e atualizada, organizando as duas redes em um quadro comparativo que evidencia convergências, diferenças e implicações práticas de suas escolhas de projeto.

Além disso, o trabalho procura manter uma abordagem didática sem abrir mão do rigor conceitual. Essa característica é especialmente importante em um tema que, muitas vezes, é apresentado de maneira excessivamente técnica ou, em sentido oposto, de forma superficial. Assim, o estudo avança ao reunir fundamentação teórica, análise individual das duas redes e comparação sistemática em uma mesma estrutura, oferecendo ao leitor uma visão mais clara sobre como Bitcoin e Ethereum se relacionam e se distinguem dentro do ecossistema *blockchain*.

1.6 Objetivos

Esta seção apresenta o objetivo geral e os objetivos específicos que orientaram o desenvolvimento deste trabalho.

1.6.1 Objetivo Geral

Analisar comparativamente as arquiteturas do Bitcoin e do Ethereum, de modo a identificar suas principais convergências, diferenças estruturais e implicações práticas no contexto da tecnologia *blockchain*.

1.6.2 Objetivos específicos

- apresentar os fundamentos técnicos da tecnologia *blockchain* e das criptomoedas;
- descrever a arquitetura do Bitcoin, com ênfase em seu modelo transacional, mecanismo de consenso, política monetária, escalabilidade e privacidade;
- descrever a arquitetura do Ethereum, considerando modelo de contas, estado global, EVM, *gas*, consenso, escalabilidade e aplicações;
- comparar Bitcoin e Ethereum a partir de critérios como filosofia de design, gestão de estado, mecanismos de consenso, escalabilidade, privacidade e espectro de aplicações;
- sintetizar os principais resultados comparativos, evidenciando como as diferenças entre essas redes refletem propostas distintas de uso da *blockchain*.

1.7 Metodologia e organização do trabalho

Do ponto de vista metodológico, este trabalho se caracteriza como uma pesquisa qualitativa de natureza descritiva e comparativa, desenvolvida por meio de revisão bibliográfica de literatura técnica e científica. As fontes consultadas incluem artigos de periódicos, trabalhos de conclusão de curso, documentação técnica oficial das redes e livros especializados, com ênfase em publicações dos últimos dez anos, complementadas por documentos seminais que fundamentam o campo, como o *whitepaper* de Nakamoto (2008) e o *Yellow Paper* de Wood (2025).

Este trabalho está organizado em quatro capítulos, além desta introdução e da conclusão. O Capítulo 2 apresenta a fundamentação teórica, abordando os conceitos essenciais relacionados à tecnologia *blockchain* e às criptomoedas. O Capítulo 3 analisa a arquitetura do Bitcoin, discutindo seu surgimento, sua estrutura de blocos, o modelo de UTXOs, o mecanismo de consenso, a política monetária, a escalabilidade

e a privacidade. O Capítulo 4 examina a arquitetura do Ethereum, com foco em sua proposta programável, no modelo de contas, na *Ethereum Virtual Machine*, no mecanismo de *gas*, na evolução do consenso e nas aplicações da rede. O Capítulo 5 desenvolve a análise comparativa entre Bitcoin e Ethereum, organizando a comparação a partir de critérios técnicos centrais. Por fim, a conclusão retoma os principais resultados obtidos e apresenta o fechamento da pesquisa.

2 FUNDAMENTOS DA BLOCKCHAIN E DAS CRIPTOMOEDAS

A compreensão de criptomoedas e de suas redes exige, primeiro, o entendimento dos fundamentos técnicos que as sustentam. Tecnologias como o *blockchain* viabilizaram que usuários realizem transações entre si sem a necessidade de uma entidade intermediária confiável, como um banco, ao combinar registro distribuído, mecanismos criptográficos e participação coletiva dos nós da rede (CHERVINSKI; KREUTZ, 2019).

Nesse contexto, a *blockchain* é frequentemente descrita como um livro-razão distribuído mantido por uma rede de computadores que verifica coletivamente transações antes de registrá-las, permitindo colaboração sem uma autoridade central (FIGUEIREDO; LIMA, 2021). O funcionamento da *blockchain* se apoia em princípios como funções *hash*, registro temporal (*timestamp*), assinaturas digitais, rede *peer-to-peer*[1] (P2P) e mecanismos de consenso para validação e geração de novos blocos, elementos que formam a base de aplicações como criptomoedas e plataformas programáveis (FIGUEIREDO; LIMA, 2021).

Historicamente, a base para essa arquitetura foi consolidada com a proposição do Bitcoin, onde a rede P2P foi introduzida como a solução para o problema de gasto duplo (NAKAMOTO, 2008). A partir dessa estrutura, a *blockchain* atua como uma estrutura de armazenamento distribuído com elevada resistência à adulteração, devido ao seu funcionamento baseado em algoritmos matemáticos. Isso permite a criação de um acervo de registros integral, inalterável e passível de auditoria de todas as operações executadas (FERGUSON, 2018 *apud* CARDOSO *et al*., 2020; ANGELIS, 2018 *apud* CARDOSO *et al*., 2020). Dessa forma, a confiança que antes era exigida de uma entidade validadora central passa a ser fundamentada na própria criptografia, sendo sustentada e conferida de forma distribuída pelos diversos computadores conectados à rede (ALVES, 2022).

Este capítulo apresenta os fundamentos técnicos que sustentam as criptomoedas e as redes *blockchain*, com o objetivo de fornecer a base conceitual necessária para a análise comparativa desenvolvida nos capítulos seguintes. Para

[1] *Peer-to-peer* (P2P), ou rede ponto a ponto, refere-se a uma arquitetura de rede distribuída onde cada computador conectado (chamado de nó ou *peer*) atua simultaneamente como cliente e servidor. Esse modelo permite o compartilhamento de dados e recursos diretamente entre os participantes, dispensando a necessidade de um servidor central para intermediar a comunicação.

isso, são abordados, de forma progressiva, o conceito de *blockchain* e sua estrutura de blocos encadeados, as funções hash criptográficas, o modelo de rede P2P e a validação distribuída, os mecanismos de consenso, com destaque para a Prova de Trabalho, o processo de mineração e seus incentivos econômicos, as chaves criptográficas, endereços e carteiras, o ciclo de vida de uma transação, as propriedades e limitações do sistema, como transparência e privacidade, e, por fim, as aplicações da *blockchain* além das criptomoedas, incluindo os contratos inteligentes.

2.1 Conceito de blockchain

As inovações tecnológicas que dão suporte às moedas digitais permitiram que as transferências de valor ocorram diretamente entre as partes interessadas. Isso eliminou a obrigatoriedade de instituições financeiras atuarem como pontes mediadoras, um fator de transformação que despertou forte atenção tanto do meio acadêmico quanto do setor empresarial (CHERVINSKI; KREUTZ, 2019).

Em termos fundamentais, a *blockchain* pode ser definida como uma estrutura de dados descentralizada, composta por um encadeamento contínuo de blocos de informações. Nessa rede, qualquer nó conectado tem a capacidade de armazenar a versão integral do histórico e participar ativamente do processo de aprovação das operações, utilizando, para isso, garantias baseadas em criptografia (CHERVINSKI; KREUTZ, 2019).

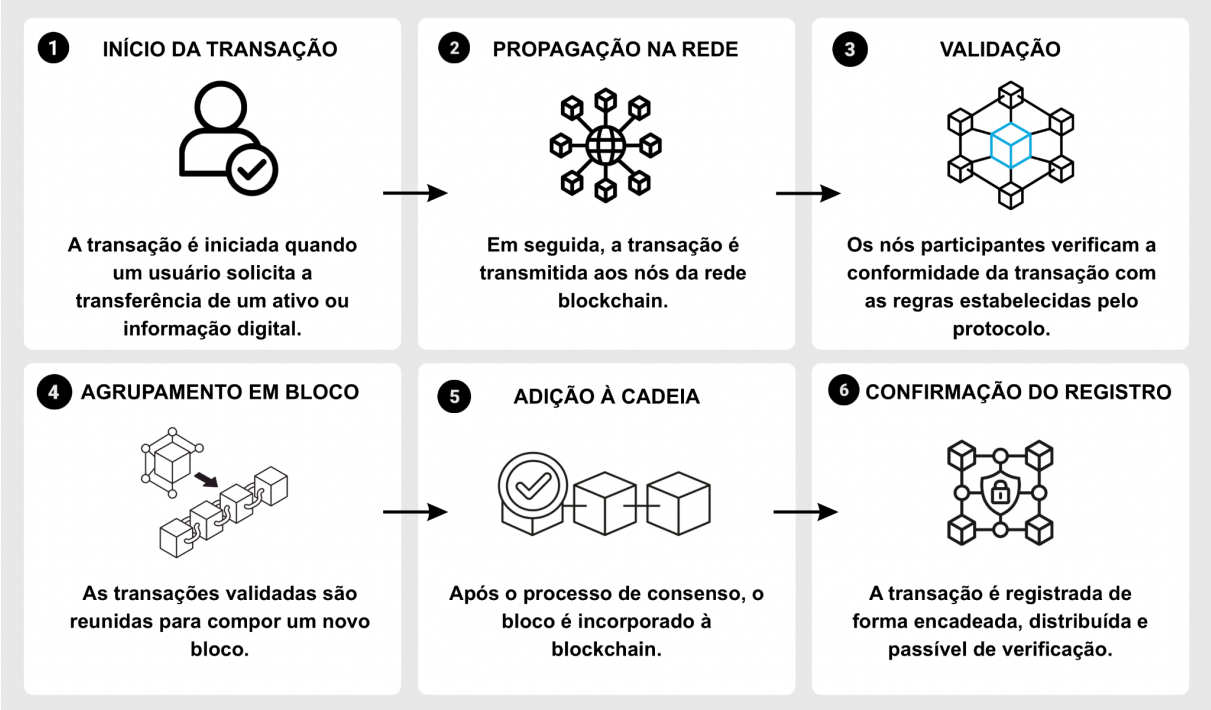
Para facilitar a compreensão, a *blockchain* é frequentemente conceituada como um grande livro contábil — ou "livro-razão distribuído" —, público e descentralizado, onde constam de forma imutável os registros de todas as operações ocorridas na rede, previamente validadas pelos próprios usuários. Diferentemente de um sistema tradicional, esse banco de dados é atualizado por nós (computadores) participantes de uma rede P2P, com base em regras de consenso e assegurado por mecanismos como a Prova de Trabalho (*Proof-of-Work* – PoW) para dissuadir ataques cibernéticos (FERREIRA; PINTO; SANTOS, 2017).

A proposta oferecida por essa tecnologia apoia-se em três pilares fundamentais: a quebra do monopólio da confiança (que deixa de pertencer a um órgão centralizador e passa a residir nos cálculos matemáticos), a capacidade de negociação direta entre as partes e a impossibilidade de reverter os registros

passados. Assim que uma transferência atinge o status de validada, ela é agrupada com outras para constituir um bloco inédito, o qual é então anexado à cadeia existente de forma permanente e inalterável (ALVES, 2022; NAKAMOTO, 2008).

Além do uso em criptomoedas, a *blockchain* provou ser uma plataforma programável altamente versátil. Sua estrutura pode ser moldada para atender a diversos setores que exijam a documentação, validação e movimentação de identidades digitais, direitos de propriedade ou até mesmo a execução autônoma de contratos inteligentes (*smart contracts*) sob um alto padrão de segurança (FERREIRA; PINTO; SANTOS, 2017; CARDOSO *et al.*, 2020).

Figura 1 – Fluxograma simplificado mostrando os 6 passos de uma transação na *blockchain*.



Fonte: Elaborado pelo autor.

2.2 Estrutura de blocos e encadeamento

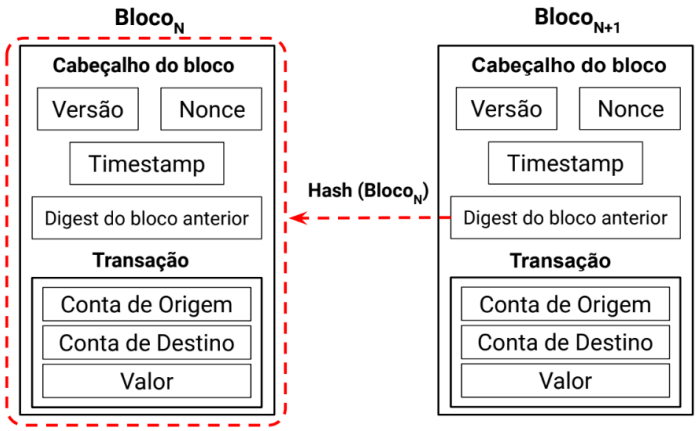
A arquitetura da *blockchain* consiste em uma sequência contínua de blocos de dados, onde cada nova unidade de informação faz uma referência direta ao bloco imediatamente anterior por meio de um identificador criptográfico exclusivo, conhecido como *hash* ou *digest*. Essa mecânica de conexão sequencial confere ao sistema uma

de suas características mais relevantes: a extrema dificuldade técnica de adulterar qualquer registro que já tenha sido consolidado na cadeia (CHERVINSKI; KREUTZ, 2019).

Para ilustrar a composição interna dessas estruturas, Chervinski e Kreutz (2019) propõem o modelo de uma aplicação bancária hipotética projetada para registrar movimentações financeiras. Nesse cenário didático, um bloco básico conteria campos específicos para garantir a ordem lógica e a segurança dos dados, tais como:

> (d_1) Versão: Versão do sistema utilizada.
> (d_2) Timestamp: Representação da data e hora de criação do bloco.
> (d_3) Nonce: Número auxiliar utilizado para realização do cálculo da função hash criptográfica.
> (d_4) Digest do bloco anterior: Resultado da aplicação de uma função hash criptográfica sobre os dados do bloco anterior.
> (d_5) Conta de origem: A conta de onde o dinheiro será retirado.
> (d_6) Conta de destino: A conta que receberá o dinheiro.
> *(d_7)* Valor da transação: Quantia de dinheiro a ser transferida. (CHERVINSKI; KREUTZ, 2019).

Figura 2 – Representação dos blocos em um *blockchain.*



Fonte: Chervinski e Kreutz (2019, p. 14).

A dinâmica visualizada na Figura 2 explicita como ocorre a interligação contínua das unidades de informação. O elo correto e inquebrável da sequência é garantido justamente porque cada novo bloco obrigatoriamente carrega dentro de si o resumo matemático do bloco anterior. Quando o algoritmo processa os dados de um bloco, ele gera uma "impressão digital" única. Esse método estabelece uma dependência criptográfica exclusiva entre as partes, blindando o sistema contra modificações

furtivas e atestando que existe apenas um histórico de registros legítimo (CHERVINSKI; KREUTZ, 2019).

O impacto dessa estrutura encadeada na segurança da rede é massivo. Se um agente malicioso tentasse fraudar os dados de uma operação passada, o identificador daquele bloco mudaria completamente. Para que a alteração passasse despercebida, o invasor teria a difícil tarefa de gerar um novo resumo que fosse compatível com a conexão do bloco seguinte; do contrário, a ligação se romperia e a inconsistência seria detectada pelos demais usuários. Para ter sucesso no ataque, o fraudador seria obrigado a refazer todo o cálculo computacional do bloco corrompido e de todos os blocos subsequentes até alcançar o topo da cadeia, uma tarefa inviabilizada pelos severos mecanismos de proteção e exigência de processamento das redes públicas (CHERVINSKI; KREUTZ, 2019).

2.3 Funções hash criptográficas e integridade dos dados

Na ciência da computação, os algoritmos de *hash* convencionais são responsáveis por receber um volume variável de informações e convertê-lo em um código alfanumérico de comprimento invariável, popularmente chamado de *digest* ou resumo criptográfico (CHERVINSKI; KREUTZ, 2019; LUCENA; HENRIQUES, 2016). Quando aplicadas ao escopo da criptografia, essas operações matemáticas atuam como vias de mão única. Para serem consideradas seguras e eficientes, elas precisam atender a requisitos rigorosos, tais como: processamento ágil para gerar o código final, inviabilidade computacional de descobrir o dado original a partir do resumo, resistência extrema contra colisões (impedindo que duas entradas diferentes gerem o mesmo resultado) e o chamado "efeito avalanche", onde uma alteração minúscula na origem modifica drasticamente todo o código resultante (CHERVINSKI; KREUTZ, 2019).

É justamente esse conjunto de características matemáticas que atesta a confiabilidade dos registros na rede. Caso um único caractere ou bit de uma transação seja modificado, o algoritmo produzirá um *hash* inteiramente distinto, evidenciando de forma imediata e irrefutável que a informação original foi corrompida (CHERVINSKI; KREUTZ, 2019). O propósito central de empregar essa técnica unidirecional é criar um mecanismo de alta resistência contra a falsificação ou adulteração de qualquer

registro digital armazenado na infraestrutura distribuída (LUCENA; HENRIQUES, 2016).

Transportando esse conceito diretamente para o funcionamento da *blockchain*, a interligação estrutural e cronológica entre os blocos é forjada exclusivamente por meio desses resumos criptográficos. Em redes pioneiras como o Bitcoin, o padrão adotado para garantir essa amarração lógica é o algoritmo SHA-256 (NAKAMOTO, 2008). Consequentemente, a inviolabilidade de toda a cadeia de dados e a sua resiliência contra fraudes cibernéticas estão intrinsecamente ancoradas na solidez dessas funções matemáticas, que atuam como os verdadeiros selos de autenticidade do sistema (CHERVINSKI; KREUTZ, 2019).

2.4 Rede P2P e validação distribuída

A tecnologia *blockchain* atua essencialmente como um banco de dados compartilhado, onde múltiplos computadores operam em conjunto para auditar e confirmar as operações antes de sua gravação definitiva. Essa dinâmica viabiliza a cooperação mútua entre os usuários, eliminando a exigência de um órgão centralizador e imparcial para mediar as relações (SCHWAB, 2016 *apud* FIGUEIREDO; LIMA, 2021). Na prática, a validação das transferências ocorre por meio do esforço conjunto dos participantes. Qualquer indivíduo conectado possui a capacidade de baixar e retransmitir a versão integral do histórico de dados, consolidando a natureza descentralizada do sistema (CHERVINSKI; KREUTZ, 2019).

O modelo de comunicação P2P é a base que permite aos usuários transacionarem valores e informações diretamente entre si, removendo definitivamente a necessidade de instituições financeiras ou outros intermediários (ALVES, 2022). Dentro dessa topologia, as máquinas interligadas — tecnicamente denominadas nós ou *peers* — operam de maneira simultânea e independente, exigindo um nível mínimo de coordenação estrutural (NAKAMOTO, 2008). A propagação de novas operações e blocos pela rede não requer que a informação chegue a todos os computadores no mesmo instante. A transmissão de dados flui de forma orgânica, operando sob o princípio de "melhor esforço" *(best effort*), no qual os nós repassam as informações aos seus pares assim que as recebem (NAKAMOTO, 2008).

A força dessa arquitetura descentralizada reside no fato de que qualquer tentativa de alteração no histórico passa pelo crivo da maioria dos participantes. Essa validação em massa atua como uma barreira de proteção robusta contra a inserção de transações fraudulentas ou dados corrompidos na cadeia principal (LUCENA; HENRIQUES, 2016). Toda essa mecânica assegura uma alta resiliência e tolerância a falhas. Os computadores podem se desconectar e retornar à rede a qualquer momento sem comprometer a integridade global; ao se reconectar, o nó simplesmente atualiza seu histórico, adotando a ramificação que contiver a maior carga de processamento matemático acumulado como o registro oficial dos eventos ocorridos durante o seu período de inatividade (NAKAMOTO, 2008).

2.5 Mecanismos de consenso e Prova de Trabalho

Em *blockchains* públicas, um problema central é controlar a criação de novos blocos e evitar que um atacante reescreva o histórico da cadeia. Para isso, um dos mecanismos mais conhecidos é a Prova de Trabalho, adotada originalmente por redes como o Bitcoin. Nesse modelo, não basta calcular o *digest* do bloco: o resultado precisa obedecer a uma restrição matemática que exige um elevado esforço computacional (CHERVINSKI; KREUTZ, 2019).

Essa restrição descrita envolve a procura por um valor cujo *hash* comece com um número específico de *bits* zero. A média de trabalho requerida cresce de forma exponencial de acordo com a quantidade de zeros exigida pela rede. Para variar a saída e tentar atender à restrição, utiliza-se um campo no bloco chamado *nonce*, que é incrementado sequencialmente até que o resultado validado seja obtido (CHERVINSKI; KREUTZ, 2019). Esse processo de resolução de funções matemáticas complexas por meio de força computacional é a base do que se denomina convencionalmente como mineração.

De acordo com Nakamoto (2008), a segurança desse mecanismo está diretamente ligada ao seu caráter descentralizado e à regra da "cadeia mais longa". Em uma rede baseada em Prova de Trabalho, a versão do histórico de transações que possuir o maior esforço computacional investido será considerada a verdadeira pelos demais participantes. Para que um atacante consiga fraudar a rede e reescrever um bloco do passado, ele teria a difícil tarefa de refazer o cálculo daquele bloco e de todos os blocos seguintes, precisando trabalhar mais rápido do que todos os nós

honestos da rede juntos. Na prática, o sistema se mantém seguro desde que os computadores honestos controlem coletivamente a maior parte do poder de processamento, tornando um ataque viável apenas se o fraudador dominar mais da metade da força computacional (situação popularmente conhecida como ataque de 51%).

Embora a Prova de Trabalho seja a base de segurança consolidada do Bitcoin, ela não é a única forma de atingir um acordo distribuído. Como o "consenso" é um tema estrutural amplo, a literatura apresenta alternativas que não dependem estritamente do elevado poder computacional. A principal delas é a prova de participação (*Proof-of-Stake* – PoS), um modelo de extrema relevância para o mercado de criptomoedas, pois representa a evolução arquitetônica adotada por redes como o Ethereum para buscar maior eficiência e escalabilidade (TSCHORSCH; SCHEUERMANN, 2016 *apud* CHERVINSKI; KREUTZ, 2019).

2.6 Mineração, criação de blocos e incentivos econômicos

Mineradores são os participantes da rede que disponibilizam sua capacidade computacional para tentar calcular os *hashes* válidos e adicionar novos blocos ao final da cadeia. Quando um usuário realiza uma transferência, os dados dessa operação são transmitidos para toda a rede, permitindo que os mineradores agrupem essas transações pendentes em um bloco candidato antes de iniciar a busca pela resolução do desafio matemático exigido pela Prova de Trabalho (CHERVINSKI; KREUTZ, 2019).

Devido ao elevado custo de hardware e energia elétrica necessário para executar a Prova de Trabalho, o sistema requer um mecanismo que encoraje os participantes a fornecerem seu poder de processamento de forma honesta para a segurança da rede. Esse incentivo ocorre de duas maneiras principais: por meio de recompensas em novas moedas e pelas taxas de transação. Por convenção, a primeira transação de um bloco (*coinbase transaction*) é uma operação especial que gera novas moedas e as entrega ao criador do bloco. Isso não apenas incentiva os nós a sustentarem a rede, mas também fornece um meio descentralizado de colocar moedas em circulação, visto que não há uma autoridade central para emiti-las (NAKAMOTO, 2008). Além disso, como os usuários podem incluir taxas voluntárias em suas transações, os mineradores tendem a priorizar as operações que oferecem

maiores recompensas financeiras para inclusão mais rápida no bloco (CHERVINSKI; KREUTZ, 2019).

A emissão dessas novas criptomoedas é rigidamente controlada pelo protocolo. No caso do Bitcoin, a recompensa concedida por bloco minerado é reduzida pela metade em intervalos regulares – especificamente a cada 210.000 blocos, evento conhecido no mercado como *halving* (redução periódica da recompensa por bloco) –, contribuindo para controlar a inflação e limitar a oferta total da moeda ao longo do tempo (CHERVINSKI; KREUTZ, 2019).

Para garantir que a emissão e a confirmação de blocos permaneçam estáveis mesmo com a entrada ou saída significativa de mineradores, o sistema possui um ajuste automático de dificuldade. Essa calibração ocorre periodicamente (a cada 2.016 blocos na rede Bitcoin) com o objetivo de manter o tempo médio de criação de um novo bloco em aproximadamente dez minutos, elevando a complexidade matemática se a rede acelerar e reduzindo-a se desacelerar (CHERVINSKI; KREUTZ, 2019).

Por fim, com o aumento exponencial da dificuldade ao longo dos anos, tornou-se uma prática comum que os mineradores se organizem em grupos cooperativos (*mining pools*). Ao trabalharem em conjunto unindo seu poder computacional, eles conseguem validar blocos com maior frequência e dividem as recompensas, obtendo um fluxo de retorno financeiro mais estável e previsível (CHERVINSKI; KREUTZ, 2019).

2.7 Chaves criptográficas, endereços e carteiras

A segurança e a autoria das transações na *blockchain* são garantidas pelo uso de criptografia assimétrica, que gera um par de chaves matematicamente vinculadas para cada usuário: uma pública e uma privada. A chave pública atua de forma semelhante a um número de conta bancária, servindo como a identidade visível para a qual os fundos são enviados. Por outro lado, a chave privada funciona como uma senha exclusiva do proprietário, que autoriza a transferência dos fundos atrelados àquela chave pública. É fundamental que a chave privada seja mantida em absoluto sigilo, pois quem a possui detém o controle total sobre os ativos (CHERVINSKI; KREUTZ, 2019).

Na arquitetura proposta para redes como o Bitcoin, uma moeda digital é essencialmente definida como uma cadeia de assinaturas digitais. Quando um usuário deseja transferir um valor, ele utiliza sua chave privada para assinar digitalmente um *hash* da transação anterior juntamente com a chave pública do próximo proprietário. Essa assinatura pode ser validada por qualquer participante da rede usando a chave pública do remetente, garantindo a autenticidade da operação sem a necessidade de expor a chave privada original (NAKAMOTO, 2008).

Para facilitar o uso e aumentar a segurança, o endereço final de recebimento não costuma ser a chave pública em seu formato bruto. O endereço é, na verdade, derivado da chave pública por meio da aplicação sequencial de algoritmos de *hashing* (como SHA-256 e RIPEMD-160). Esse processo resulta em um código alfanumérico menor e padronizado, embora os usuários ainda possuam a opção técnica de utilizar a própria chave pública diretamente como endereço (TSCHORSCH; SCHEUERMANN, 2016 *apud* CHERVINSKI; KREUTZ, 2019).

Para gerenciar toda essa infraestrutura criptográfica, utilizam-se os softwares conhecidos como carteiras virtuais (wallets). Diferente do conceito tradicional, uma *wallet* não armazena as criptomoedas em si — visto que os saldos são apenas registros imutáveis na *blockchain* —, mas atua como um gerenciador das chaves e endereços do usuário. Como prática de privacidade e organização, as carteiras modernas criam automaticamente novos endereços para cada transação e para o recebimento de troco, permitindo que um único usuário administre múltiplos endereços de forma transparente e simplificada (CHERVINSKI; KREUTZ, 2019).

2.8 O ciclo de vida de uma transação

A estrutura fundamental de uma transferência em redes *blockchain* baseia-se na indicação de endereços de origem e de destino. Quando um usuário deseja realizar um pagamento, ele utiliza os registros da rede para provar a origem dos seus fundos e define o endereço público do destinatário para o qual o valor será transferido, incluindo também uma taxa de transação voluntária que servirá de incentivo aos mineradores (CHERVINSKI; KREUTZ, 2019).

Independentemente do modelo de contabilização de saldo adotado pela rede, o ponto central para garantir a segurança, a autenticidade e o não repúdio das operações é o uso de esquemas de assinaturas digitais, frequentemente baseados

em algoritmos como o Algoritmo de Assinatura Digital por Curva Elíptica (*Elliptic Curve Digital Signature Algorithm – ECDSA*). Essas assinaturas criptográficas são essenciais para assegurar a validade das operações, pois garantem que somente o detentor da chave privada correspondente possa autorizar a movimentação dos fundos vinculados àquele endereço (SENDIN; MIANI; RIBEIRO, 2024).

O processo operacional se inicia quando o remetente cria uma mensagem contendo os dados da transferência e gera a assinatura exclusiva. Feito isso, ele transmite para a rede a mensagem, a respectiva assinatura e a sua chave pública. A verificação de legitimidade dessa movimentação ocorre de forma puramente matemática e descentralizada. O receptor (ou qualquer nó participante da rede) realiza uma operação utilizando a chave pública e a assinatura recebidas. Esse cálculo confirma se a assinatura foi de fato gerada pela chave privada correspondente, sem que a mesma precise ser exposta em momento algum (CHERVINSKI; KREUTZ, 2019).

Por fim, a consolidação da transferência depende da arquitetura P2P. Após assinar a transação, o remetente a dissemina (propaga) para os computadores conectados. As transações recém-chegadas são verificadas pelos participantes e repassadas em regime de melhor esforço (*best effort*). Os nós validadores da rede coletam essas transações pendentes, as acumulam e as organizam em um bloco candidato. A partir desse momento, inicia-se o processo de consenso da rede; assim que o bloco válido é gerado e adicionado à cadeia principal, a transação é confirmada e registrada no histórico imutável (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019).

2.9 Transparência, privacidade e bifurcações

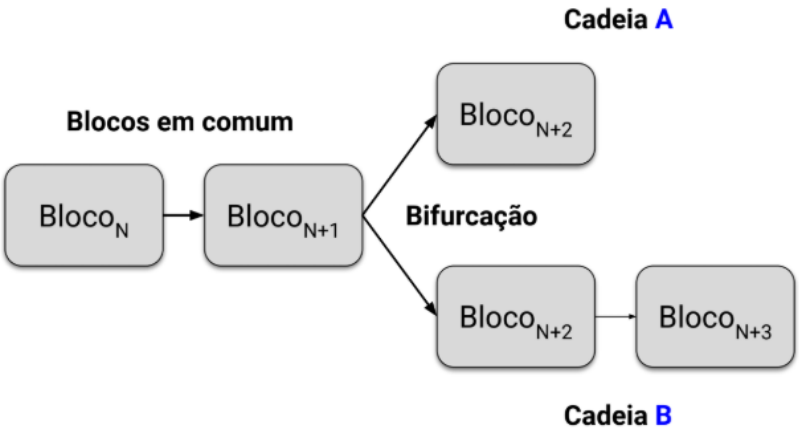
Uma das propriedades mais marcantes das *blockchains* públicas, como o Bitcoin, é a sua total transparência. O histórico completo de todas as operações e o fluxo de transações ficam disponíveis de forma aberta para qualquer participante da rede. Por conta dessa exposição estrutural, autores como Sendin, Miani e Ribeiro (2024) classificam essas redes como sistemas "pseudoanônimos", e não completamente anônimos. Embora os nomes reais não estejam registrados na cadeia, a transparência permite que técnicas de análise forense e heurísticas de clusterização rastreiem o fluxo financeiro, possibilitando a correlação matemática entre diferentes

endereços e, eventualmente, a identificação das identidades reais por trás das operações (CHERVINSKI; KREUTZ, 2019; SENDIN; MIANI; RIBEIRO, 2024).

Para mitigar essa vulnerabilidade e tentar preservar a privacidade dos usuários em um ambiente tão transparente, o modelo de segurança do protocolo sugere a quebra proposital do fluxo de informações. A prática recomendada é a geração de um novo par de chaves (um novo endereço público) para cada transação recebida. Dessa forma, evita-se que múltiplas operações sejam vinculadas a um único proprietário, dificultando o rastreio do saldo total e do comportamento financeiro do indivíduo pela rede (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019).

Outra característica inerente à natureza distribuída dessas redes é a possibilidade de ocorrência de bifurcações temporárias, conhecidas como *forks*. Esse fenômeno acontece, geralmente, devido ao tempo natural de propagação das informações pela rede global. É estatisticamente possível que dois participantes (mineradores) encontrem a solução matemática para um bloco válido de forma quase simultânea. Quando isso ocorre, diferentes nós podem receber e adotar blocos distintos em momentos diferentes, fazendo com que a *blockchain* se divida temporariamente em duas ramificações válidas (CHERVINSKI; KREUTZ, 2019).

Figura 3 – Bifurcação na cadeia de blocos.



Fonte: Chervinski e Kreutz, 2019.

A resolução dessa situação é gerida de forma autônoma pelo protocolo por meio da "regra da cadeia mais longa". À medida que novos blocos são criados, uma das ramificações acumulará mais poder de trabalho e se tornará mais longa do que a outra. O sistema, então, orienta que todos os nós da rede adotem imediatamente a cadeia de maior extensão como a verdadeira e definitiva. A ramificação mais curta deixa de ser considerada a cadeia principal e as transações nela contidas que não haviam sido incluídas na cadeia principal retornam automaticamente ao conjunto de transações pendentes, aguardando confirmação nos próximos blocos (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019).

2.10 Aplicações da blockchain além das criptomoedas

Embora o objetivo inicial do desenvolvimento da *blockchain* tenha sido viabilizar a criação de criptomoedas descentralizadas, como o Bitcoin, a literatura técnica demonstra que a tecnologia possui um potencial arquitetônico muito maior. Suas propriedades de segurança e imutabilidade abrem caminho para aplicações que vão além da simples transferência de moedas digitais (FIGUEIREDO; LIMA, 2021).

Estudos de mapeamento sistemático apontam que essa infraestrutura descentralizada pode ser aplicada em diversas indústrias onde seja estritamente necessário registrar, confirmar e transferir propriedades ou direitos. Isso consolida a visão da *blockchain* como uma tecnologia robusta de gerenciamento de dados aplicável a setores além do financeiro, abrangendo áreas como governança, logística e, principalmente, o campo jurídico e contratual (FERREIRA; PINTO; SANTOS, 2017; CARDOSO *et al*., 2020).

Nesse cenário de expansão de uso, surge o que se classifica como a "segunda geração" da *blockchain*. O principal expoente dessa fase é a rede Ethereum, descrita como uma tecnologia que transcende a transferência de valores ao permitir a execução de programas autoexecutáveis dentro de seus blocos. Essa inovação técnica viabilizou a criação de códigos que realizam atividades específicas de forma autônoma conforme termos pré-programados, estruturas estas que receberam o nome de contratos inteligentes (MASCARENHAS, 2018 *apud* FIGUEIREDO; LIMA, 2021).

De forma didática, os contratos inteligentes são definidos como programas computacionais compostos por algoritmos que executam automaticamente os termos

de um acordo assim que as condições pré-programadas são satisfeitas. Para ilustrar esse funcionamento, utiliza-se frequentemente a clássica analogia da máquina de venda automática (*vending machine*), proposta originalmente na década de 1990: uma vez que o cliente insere o pagamento e seleciona o produto, a máquina processa a transação e libera o item de forma mecânica e determinística, sem a necessidade de um intermediário humano para aprovar ou realizar a troca (SZABO, 1997 *apud* FIGUEIREDO; LIMA, 2021). Na *blockchain*, esse mecanismo garante que acordos digitais sejam cumpridos de forma automática, transparente e com menor dependência de intermediários.

3 A ARQUITETURA DO BITCOIN

Neste capítulo, será analisada a arquitetura do Bitcoin, a primeira e mais consolidada rede descentralizada desse ecossistema. O objetivo é compreender o funcionamento estrutural dessa tecnologia, explorando desde a sua concepção inicial para solucionar o problema do gasto duplo até o seu modelo particular de contabilização de saldos. Além disso, serão abordadas as suas regras de política monetária, o seu sistema de consenso distribuído e as limitações intencionais de sua linguagem de programação — fatores fundamentais para o entendimento das restrições da rede e que, posteriormente, motivaram o surgimento de novas plataformas programáveis, como o Ethereum.

3.1 O surgimento do Bitcoin e o problema do gasto duplo

A fundação do mercado de criptomoedas como é conhecido hoje ocorreu no final do ano de 2008, em pleno auge da crise financeira global, um período marcado pela redução da confiança nas instituições bancárias tradicionais (NORMAN, 2020). Nesse cenário de instabilidade, foi publicado um artigo acadêmico intitulado "*Bitcoin: A Peer-to-Peer Electronic Cash System*", assinado sob o pseudônimo Satoshi Nakamoto. O propósito central do documento era propor um sistema de dinheiro eletrônico totalmente P2P, que permitisse o envio de pagamentos online diretamente de uma parte à outra sem a necessidade de tramitar por uma instituição financeira intermediária (NAKAMOTO, 2008).

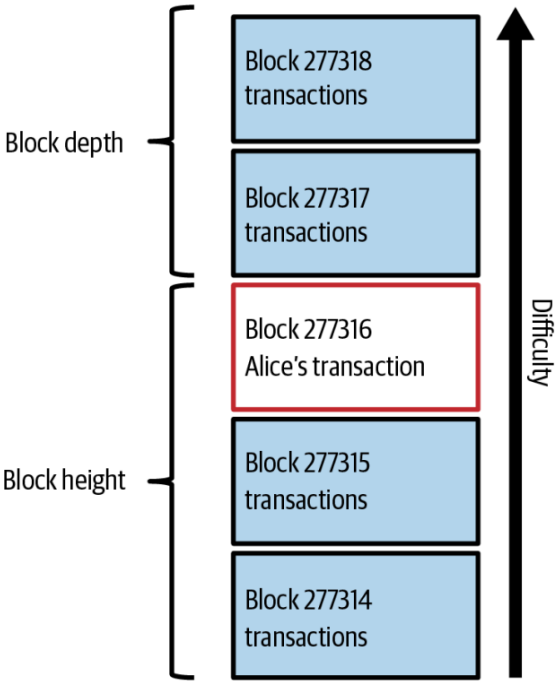
Para compreender a inovação arquitetônica proposta por esse sistema, é necessário entender o maior desafio da criação de um dinheiro digital até então: o problema do "gasto duplo". No mundo virtual padrão, quando um usuário envia um arquivo digital para outra pessoa — como uma fotografia ou um documento de texto —, ele não está entregando o arquivo original, mas sim enviando uma cópia e retendo a matriz em seu computador. Se esse mesmo princípio fosse aplicado a uma moeda digital, um indivíduo poderia simplesmente copiar o arquivo do seu dinheiro e gastar o mesmo valor infinitas vezes. Historicamente, a única forma de evitar essa fraude de duplicação era depender de um servidor central, como um banco, para registrar os saldos e descontar o valor da conta do remetente a cada transferência (ANTONOPOULOS; HARDING, 2023).

A grande ruptura tecnológica apresentada por Nakamoto (2008) foi exatamente resolver o problema do gasto duplo sem precisar confiar em um banco centralizador. Em vez de utilizar um servidor privado, a solução combinou assinaturas criptográficas com uma rede distribuída. Nesse modelo, é a própria rede global de computadores que atua como um grande livro-razão público e como um servidor de data e hora distribuído (*timestamp server*), carimbando e auditando a ordem cronológica exata das transações para atestar quem possui qual moeda. Isso tornou impossível que um usuário gastasse a mesma moeda duas vezes, pois o coletivo de máquinas rejeitaria a segunda tentativa instantaneamente ao constatar no histórico público que aquele valor já havia mudado de dono (NAKAMOTO, 2008).

A implementação prática dessa teoria consolidou-se em janeiro de 2009, quando o *software* entrou oficialmente em operação com a mineração do seu primeiro bloco, eternizado na literatura como o Bloco Gênese (ou Bloco 0). A partir desse marco, o Bitcoin demonstrou que o conceito de escassez digital e de transferência descentralizada de valor era tecnicamente viável em escala global (ANTONOPOULOS; HARDING, 2023).

Após a criação do bloco gênese, as transações passaram a ser agrupadas em blocos sucessivos, encadeados criptograficamente, formando a *blockchain*. A Figura 4 exemplifica essa estrutura ao apresentar uma transação inserida em um bloco específico da cadeia, evidenciando a organização sequencial dos blocos e o conceito de confirmações ao longo da rede (ANTONOPOULOS; HARDING, 2023, p. 27).

Figura 4 – Inclusão de uma transação em um bloco da *blockchain.*



Fonte: Antonopoulos e Harding (2023, p. 27).

3.2 A estrutura dos blocos, do blockchain e da rede P2P

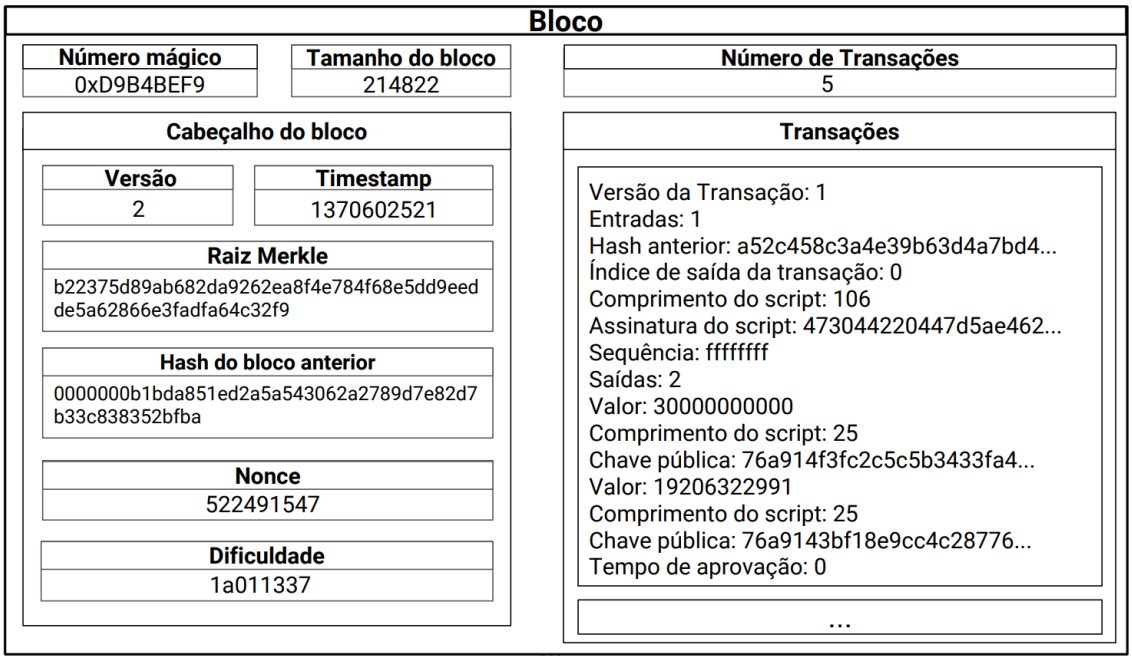
Como discutido na seção anterior, o registro histórico do Bitcoin teve início com a mineração do Bloco Gênese. A partir dele, a rede passou a organizar as transações em blocos sucessivos, que constituem a unidade fundamental de registro do sistema. Em termos conceituais, um bloco pode ser compreendido como uma página de um grande livro-razão público e distribuído, na qual são agrupadas, registradas e validadas as transações mais recentes da rede. Estruturalmente, cada bloco é composto por duas partes principais: o corpo, que contém a lista das transações incluídas naquele intervalo, e o cabeçalho (*block header*), que reúne os metadados necessários para a identificação, validação e encadeamento do bloco no restante da cadeia (ANTONOPOULOS; HARDING, 2023).

Entre os principais campos presentes no cabeçalho estão a versão do bloco, o *timestamp*, a raiz de Merkle (*Merkle root*), o hash do bloco anterior, o alvo de dificuldade e o *nonce*. Esses elementos não armazenam diretamente todas as transações, mas sintetizam as informações essenciais para que os participantes da rede possam verificar a integridade do bloco e sua posição dentro do *blockchain*.

Desse modo, o cabeçalho funciona como uma estrutura compacta de controle, enquanto o corpo armazena os dados transacionais propriamente ditos.

> (c_1) Número mágico: Valor utilizado para identificar o tipo de estrutura contida nos dados. Neste caso, um bloco. Este valor é específico do protocolo Bitcoin.
> (c_2) Tamanho do bloco: Especifica o tamanho em *bytes* dos dados contidos no bloco.
> (c_3) Cabeçalho do bloco: Contém dados que identificam o bloco atual.
> (c_4) Versão: Especifica a versão do sistema no momento da criação do bloco.
> (c_5) *Timestamp*: Representa o momento no tempo em que o bloco foi criado.
> (c_6) Raiz Merkle: Um tipo de *hash* utilizado para verificar a validade das transações contidas nos blocos sem a necessidade de verificar todas as informações das transações. Para realizar a verificação é necessário o cabeçalho dos blocos e uma estrutura chamada de Árvore de Merkle
> *(c_7) Nonce*: campo cujo valor deve ser modificado até que o *digest* resultante do bloco atenda as exigências do sistema.
> *(c_8)* Dificuldade*: Especifica o número de bits 0 necessários à esquerda do digest do bloco para que ele atenda às exigências do sistema.*
> *(c_9)* Número de transações: *Contém o número de transações presentes no bloco atual.*
> *(c_{10})* Transações: Contém os dados de cada uma das transações contidas no bloco. (CHERVINSKI; KREUTZ, 2019).

Figura 5 – Estrutura de um bloco do blockchain do sistema Bitcoin.



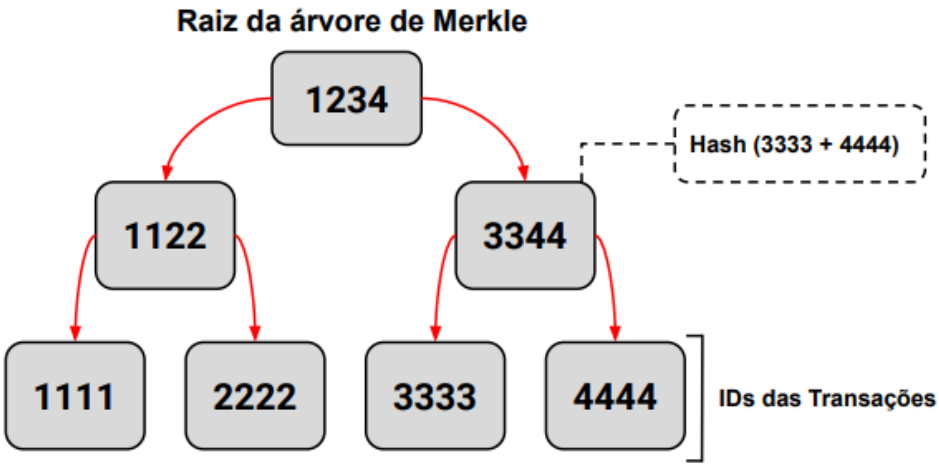
Fonte: Chervinski e Kreutz (2019, p. 21).

A Figura 5 ilustra essa organização interna ao evidenciar a separação entre os campos do cabeçalho e o conjunto de transações incluídas no bloco. Essa distinção é importante porque permite que o protocolo concentre, no cabeçalho, apenas os

elementos indispensáveis à validação criptográfica e ao encadeamento dos blocos, preservando eficiência no processamento e na verificação das informações.

Entre os elementos mais relevantes do cabeçalho está a raiz de Merkle, responsável por resumir criptograficamente todas as transações presentes no corpo do bloco. Para isso, o Bitcoin utiliza uma estrutura denominada Árvore de Merkle (*Merkle Tree*), na qual os identificadores das transações são agrupados em pares e submetidos a sucessivas operações de hash até resultar em um único valor no topo da árvore. Esse valor final, inserido no cabeçalho, funciona como um resumo criptográfico de todo o conjunto de transações daquele bloco. Assim, em vez de registrar cada transação individualmente no cabeçalho, o sistema armazena apenas a raiz de Merkle, tornando a estrutura mais compacta e eficiente (CHERVINSKI; KREUTZ, 2019).

Figura 6 – Representação de uma Árvore de Merkle.

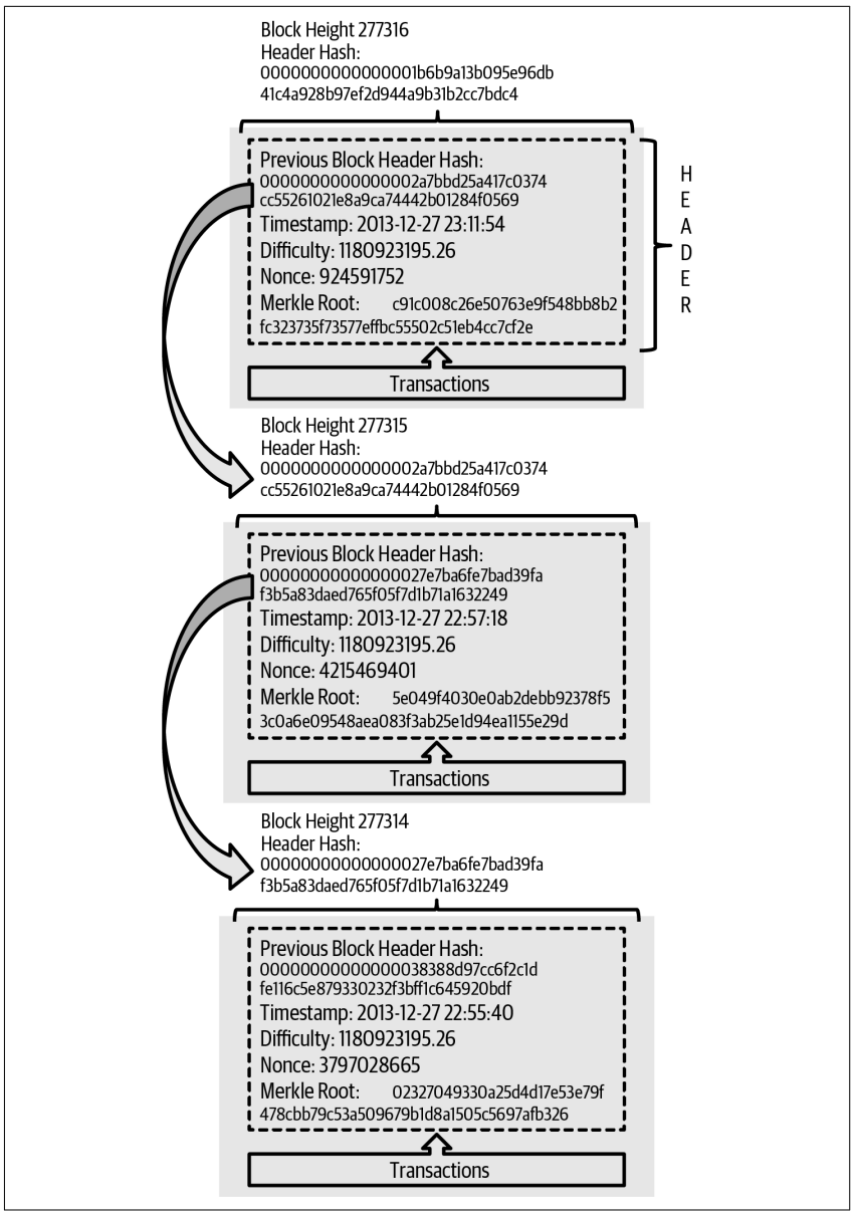


Fonte: Chervinski e Kreutz (2019, p. 21).

A Figura 6 representa esse processo de sumarização. Nos nós-folha da árvore estão os identificadores das transações, enquanto os nós superiores armazenam os *hashes* resultantes da combinação dos níveis inferiores, até que se obtenha a raiz de Merkle. Essa arquitetura permite verificar a integridade de uma transação específica sem a necessidade de recalcular ou examinar todas as demais transações do bloco. Em termos práticos, isso reduz o custo computacional das verificações e favorece a escalabilidade e a auditabilidade da rede, uma vez que um grande conjunto de transações pode ser representado por um único código de 32 *bytes* no cabeçalho do bloco (CHERVINSKI; KREUTZ, 2019; ANTONOPOULOS; HARDING, 2023).

A característica de imutabilidade do *blockchain* decorre justamente da forma como os blocos são conectados entre si. No cabeçalho de cada novo bloco minerado é incluído, obrigatoriamente, o hash do cabeçalho do bloco anterior. Esse mecanismo estabelece uma ligação criptográfica contínua entre os blocos, formando a cadeia de blocos propriamente dita. Como consequência, qualquer alteração em uma transação registrada em um bloco anterior modificaria a raiz de Merkle e, por extensão, o *hash* daquele bloco, rompendo a consistência criptográfica dos blocos subsequentes. Para que uma fraude desse tipo fosse bem-sucedida, seria necessário recalcular todos os blocos posteriores a partir do ponto alterado, o que torna esse tipo de ataque computacionalmente impraticável em condições normais da rede (ANTONOPOULOS; HARDING, 2023).

Figura 7 – Blocos conectados em uma cadeia, cada um referenciando o *hash* do cabeçalho do bloco anterior.



Fonte: Antonopoulos e Harding (2023, p. 251).

A Figura 7 evidencia essa lógica de encadeamento, mostrando que cada bloco depende criptograficamente do anterior. Dessa forma, a confiabilidade do registro não decorre de um controle centralizado, mas da própria estrutura matemática que vincula cada novo bloco ao histórico previamente consolidado.

Entretanto, para que essa arquitetura funcione de forma descentralizada e resistente à censura, ela não pode depender de um servidor central. É nesse contexto que a rede P2P se torna um componente essencial do Bitcoin. Em vez de operar sob

o modelo tradicional cliente-servidor, o sistema é mantido por uma rede distribuída de computadores independentes, denominados nós, que se comunicam entre si de forma horizontal e sem uma autoridade central de controle (NAKAMOTO, 2008).

Esses nós desempenham funções como armazenar cópias do *blockchain*, validar transações e blocos e retransmitir informações pela rede. Quando uma nova transação é criada ou quando um novo bloco é minerado, a informação é propagada entre os nós vizinhos, que verificam sua validade e a retransmitem aos demais participantes. Esse processo de disseminação, frequentemente descrito como um mecanismo de propagação do tipo *gossip*, permite que os dados se espalhem rapidamente pela rede e que os participantes mantenham cópias sincronizadas do livro-razão distribuído (ANTONOPOULOS; HARDING, 2023).

Assim, a segurança e a robustez do Bitcoin decorrem da combinação entre três elementos complementares: a estrutura interna dos blocos, que organiza e resume criptograficamente as transações; o encadeamento por *hashes*, que protege a integridade do histórico; e a rede P2P, que assegura a distribuição, a validação e a replicação dessas informações sem a necessidade de uma entidade central intermediadora.

3.3 O modelo de transações baseado em UTXOs

Para compreender a dinâmica financeira da rede, é necessário distinguir esse modelo da lógica tradicional de contas bancárias. Em sistemas financeiros convencionais, um usuário possui um saldo único e centralizado que é incrementado ou deduzido a cada operação. No entanto, a arquitetura do Bitcoin não registra saldos unificados em contas. Em vez disso, o sistema baseia-se em um modelo de "Saídas de Transações Não Gastas", tecnicamente denominado *Unspent Transaction Output* (UTXO) (ANTONOPOULOS; HARDING, 2023).

Para fins didáticos, o funcionamento das UTXOs assemelha-se fortemente à mecânica transacional do dinheiro físico. Se um indivíduo possui uma única cédula de R$ 50,00 e deseja adquirir um produto que custa apenas R$ 10,00, ele não possui a capacidade de "rasgar" a nota e entregar somente a fração correspondente ao pagamento. Ele é obrigado a repassar a cédula inteira de R$ 50,00 (a entrada, ou *input*) e, em contrapartida, receberá R$ 40,00 de troco (a nova saída, ou *output*) (NORMAN, 2020).

Na rede Bitcoin, a lógica computacional é rigorosamente idêntica: não é possível fracionar um registro de recebimento anterior. Uma nova transação consome a entrada (*input*) original em sua totalidade e gera novas saídas (*outputs*). Geralmente, cria-se uma saída destinada ao endereço do recebedor com o valor do pagamento exato, e outra saída devolvida ao próprio emissor, que representa o troco da operação (ANTONOPOULOS; HARDING, 2023; SENDIN; MIANI; RIBEIRO, 2024).

Dessa forma, o "saldo" de um usuário não é um valor estático armazenado em um banco de dados, mas sim a soma de todas as frações de UTXOs dispersas e validadas pela *blockchain* que a sua chave privada tem o direito criptográfico de movimentar. No exato momento em que uma UTXO é usada em uma nova transferência, o seu estado no sistema é alterado para "gasta" (*Spent Transaction Output* - STXO). A partir desse instante, aquele registro é permanentemente invalidado para qualquer uso futuro por todos os nós da rede, o que atua como a barreira definitiva contra a fraude de duplicação de gastos (ANTONOPOULOS; HARDING, 2023).

Além do mecanismo de transferência, o modelo UTXO introduz propriedades específicas no que tange à privacidade e à economia do sistema. Do ponto de vista da privacidade, as carteiras modernas de Bitcoin são programadas para evitar a reutilização de endereços. Quando a transação gera o "troco", esse valor não retorna obrigatoriamente para o endereço de origem, mas é frequentemente direcionado para um endereço recém-criado e controlado pelo mesmo usuário, o que dificulta o rastreamento do fluxo de capital por agentes de análise de dados (PIMENTEL, 2017).

Outro aspecto técnico fundamental derivado dessa arquitetura é a forma como as taxas de mineração (*miner fees*) são calculadas. Diferentemente de sistemas tradicionais onde a tarifa de transferência é um campo cobrado à parte, no protocolo Bitcoin a taxa é implícita. Ela é definida matematicamente pela diferença entre o valor total das entradas e o valor total das saídas. Se uma transação consome uma entrada de maior valor do que a soma das saídas geradas, o valor residual não contabilizado é automaticamente reivindicado pelo minerador que validar o bloco, servindo como incentivo financeiro para a manutenção da segurança da rede (NAKAMOTO, 2008).

Por fim, sob a ótica da ciência da computação, o modelo UTXO opera de forma "sem estado" (*stateless*). Isso significa que cada transação é um evento isolado e independente, permitindo que os nós da rede validem múltiplas transações simultaneamente em paralelo, o que garante alta resiliência e previsibilidade

matemática. Contudo, essa mesma característica impõe severas restrições à criação de lógicas de programação complexas. Como o sistema não consegue armazenar e atualizar o "estado" contínuo de uma variável de forma maleável, torna-se inviável a execução de contratos inteligentes complexos (*Smart Contracts*), limitação estrutural que, anos mais tarde, justificaria o desenvolvimento de novas arquiteturas computacionais para sanar essa lacuna (ANTONOPOULOS; HARDING, 2023).

3.4 Mineração e consenso por Prova de Trabalho

Para manter o ecossistema funcionando de forma totalmente distribuída e sem um coordenador central, a rede Bitcoin utiliza um mecanismo de consenso denominado PoW. Na prática, esse sistema dita as regras sobre como os novos blocos de transações são confirmados, selados e adicionados ao livro-razão de forma praticamente irreversível após confirmações sucessivas (NAKAMOTO, 2008).

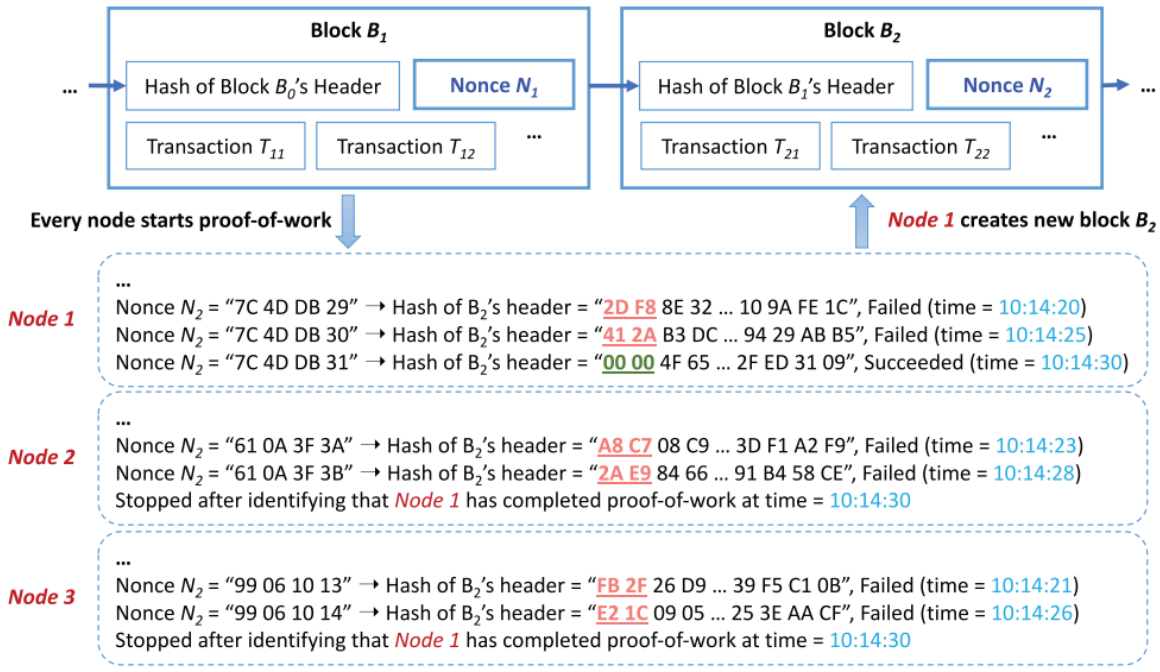
O processo de mineração, embora frequentemente descrito por meio de conceitos matemáticos densos, pode ser compreendido de forma didática como uma grande "loteria computacional". Quando um conjunto de novas transações está pronto para ser empacotado em um bloco, os computadores da rede (os mineradores) começam a competir entre si para resolver um enigma criptográfico. Esse desafio consiste em encontrar um número aleatório específico, denominado *nonce*, que, ao ser processado juntamente com os dados das transações, gere um código *hash* final que cumpra os rígidos requisitos de dificuldade exigidos pelo protocolo (ANTONOPOULOS; HARDING, 2023).

A natureza desse enigma não permite atalhos lógicos. A única maneira de encontrar o resultado correto é por meio de força bruta, o que exige um elevado poder computacional para que o *hardware* tente milhões, ou até trilhões, de combinações aleatórias por segundo. O primeiro minerador a adivinhar a solução correta ganha o direito exclusivo de selar o bloco e transmiti-lo aos demais participantes. Como contrapartida por esse esforço computacional e pela energia elétrica consumida, o vencedor recebe a recompensa do bloco em moedas recém-criadas, bem como as taxas voluntárias anexadas às transações pelos usuários (NORMAN, 2020; ANTONOPOULOS; HARDING, 2023).

Esse alto gasto de energia elétrica e capacidade de processamento não é uma ineficiência acidental, mas sim um dos principais pilares de segurança do sistema.

Uma vez que o custo físico e financeiro com equipamentos e eletricidade para participar dessa validação é extremamente elevado, torna-se economicamente irracional e impraticável para um agente malicioso tentar fraudar o registro. Para conseguir reverter uma transação confirmada no passado, um atacante teria de refazer o enorme trabalho matemático daquele bloco e de todos os blocos subsequentes, correndo contra o poder de processamento combinado de todos os nós honestos espalhados pelo globo (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019).

Figura 8 – Exemplo do mecanismo de nonce no protocolo de prova de trabalho.



Fonte: Kuo, Kim e Ohno-Machado (2017, p. 1213).

A Figura 8 ilustra, de forma visual, o mecanismo de PoW baseado no nonce. Na parte superior, observa-se que cada bloco contém o hash do bloco anterior, as transações e um campo adicional denominado nonce. Durante a mineração do bloco seguinte, diferentes nós da rede testam sucessivos valores para esse nonce, gerando novos hashes a cada tentativa. No corpo da figura, as linhas associadas aos nós mostram que a maior parte das tentativas falha, pois os hashes obtidos não atendem ao critério exigido pelo protocolo. No exemplo apresentado, o Nó 1 encontra primeiro um resultado válido, o que lhe permite criar o novo bloco e propagá-lo à rede. Em seguida, os demais nós interrompem suas tentativas para aquele bloco específico. A figura também evidencia que a segurança do processo decorre do alto custo de gerar a solução por tentativa e erro, ao passo que sua verificação é simples. Além disso, como cada bloco incorpora o hash do bloco anterior, qualquer alteração em um bloco já registrado exigiria o recálculo dos blocos subsequentes, tornando a fraude computacionalmente muito onerosa (KUO; KIM; OHNO-MACHADO, 2017).

No Bitcoin, esse processo ocorre por meio do hash repetido do cabeçalho do bloco candidato. O minerador altera o nonce até obter um hash numericamente inferior ao target definido pela rede. Como não existe um atalho para prever previamente esse resultado, a única estratégia viável é realizar tentativas sucessivas até que um valor

válido seja encontrado, o que caracteriza a PoW como um mecanismo custoso para gerar, mas simples para verificar (ANTONOPOULOS; HARDING, 2023).

3.5 A política monetária do Bitcoin e o halving

Diferentemente das moedas estatais fiduciárias, cuja emissão é controlada por bancos centrais que podem imprimir dinheiro de forma ilimitada, a política monetária do Bitcoin é estritamente governada por regras matemáticas imutáveis inscritas em seu código-fonte. A principal dessas regras estabelece uma escassez digital absoluta: o sistema foi programado para emitir um teto máximo de 21 milhões de unidades da moeda. Essa previsibilidade estrutural garante que a rede possua uma característica inerentemente deflacionária a longo prazo (ANTONOPOULOS; HARDING, 2023).

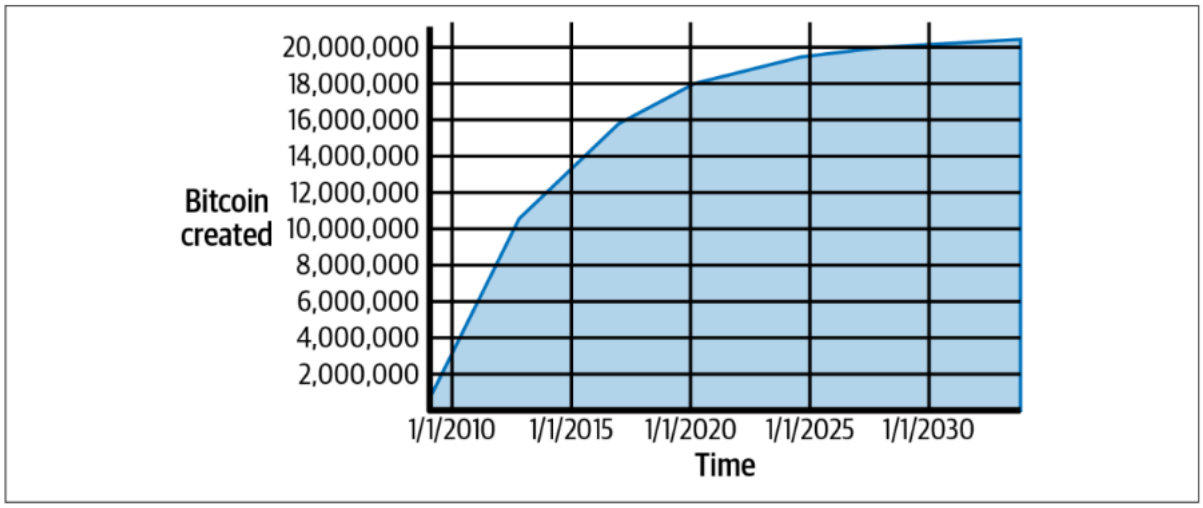
A introdução de novas moedas em circulação ocorre exclusivamente por meio do processo de validação da rede. Como incentivo financeiro para os computadores que emprestam poder de processamento para auditar e selar um novo bloco de transações, o protocolo gera e entrega a esse minerador uma quantidade predeterminada de bitcoins recém-criados. Para fins de compreensão, a literatura frequentemente compara esse processo à extração de metais preciosos no mundo físico. Tal como uma mina de ouro que, no início, oferece grandes pepitas com pouco esforço e, com o passar dos anos, exige cada vez mais trabalho para extrair frações cada vez menores, a emissão do Bitcoin foi projetada para ser decrescente ao longo do tempo (NORMAN, 2020; ANTONOPOULOS; HARDING, 2023).

Essa redução gradativa da emissão é controlada por um evento programado na arquitetura da rede conhecido como *Halving*. O protocolo estipula que, a cada 210.000 blocos minerados — o que ocorre em um intervalo de tempo aproximado de quatro anos —, a recompensa concedida aos mineradores é cortada exatamente pela metade (CHERVINSKI; KREUTZ, 2019).

Quando a rede foi lançada em 2009, a recompensa inicial era de 50 bitcoins por bloco. Após sucessivos eventos de *halving*, essa taxa de emissão vem caindo drasticamente, criando uma curva de fornecimento previsível e transparente para todos os participantes. Essa progressão geométrica decrescente continuará a operar autonomamente até que a recompensa por bloco atinja zero, o que está matematicamente previsto para ocorrer por volta do ano de 2140, momento em que o

limite de 21 milhões será definitivamente atingido (NAKAMOTO, 2008; ANTONOPOULOS; HARDING, 2023), conforme ilustrado na Figura 9.

Figura 9 – Curva de fornecimento controlado do Bitcoin e impacto dos eventos de *halving.*



Fonte: Antonopoulos e Harding (2023, p. 265).

3.6 Escalabilidade no Bitcoin e a Lightning Network

Apesar de a arquitetura descentralizada do Bitcoin garantir alto nível de segurança e imutabilidade, ela impõe um severo limite técnico à sua capacidade de processamento. Para assegurar que computadores comuns em todo o mundo consigam sincronizar a rede, o tamanho de cada bloco e o tempo para a sua criação foram mantidos intencionalmente restritos. Como consequência, a rede principal do Bitcoin (Camada 1) consegue processar, em média, apenas sete transações por segundo. Em momentos de alta adoção e tráfego intenso, as transações acumulam-se em uma área de espera denominada *Mempool* (piscina de memória). Quando isso ocorre, o sistema transforma-se em um mercado de leilão, onde os usuários são obrigados a pagar taxas (*fees*) cada vez mais elevadas para convencer os mineradores a priorizarem as suas operações (GÜNDLACH *et al.*, 2024).

Para resolver esse gargalo sem sacrificar a segurança da rede base, a comunidade de desenvolvedores optou por não alterar o protocolo original, mas sim desenvolver soluções de "Segunda Camada" (*Layer 2*). A principal inovação nesse sentido foi a proposta da *Lightning Network*, uma rede descentralizada que opera

sobre a *blockchain* do Bitcoin, desenhada especificamente para processar micropagamentos de forma instantânea e com taxas praticamente nulas (POON; DRYJA, 2016).

A lógica de funcionamento da *Lightning Network* baseia-se na criação de canais de pagamento bidirecionais entre os usuários, permitindo que o valor transite fora da rede principal (*off-chain*). De forma didática, esse modelo assemelha-se a abrir uma "conta no bar". Quando um cliente chega a um estabelecimento, em vez de passar o cartão de crédito a cada bebida que consome — o que geraria dezenas de recibos e taxas de processamento —, ele registra um cartão no início da noite (abre o canal). Durante várias horas, ele consome livremente, e o barman apenas anota as alterações no saldo em um bloco de notas local. No final da noite, a conta é encerrada e o cartão é passado apenas uma vez, cobrando o valor total definitivo (NORMAN, 2020).

Na rede *Lightning*, o princípio é idêntico. Dois participantes ancoram um saldo inicial em um contrato inteligente na *blockchain* do Bitcoin (abertura do canal). A partir desse momento, podem realizar milhares de microtransações instantâneas entre si, alterando os saldos localmente por meio de assinaturas criptográficas, sem sobrecarregar a *Mempool*. Apenas quando decidem fechar o canal é que o saldo final líquido é transmitido e registrado de forma definitiva na *blockchain* principal. Essa engenharia permite que o Bitcoin escale para milhões de transações por segundo, mantendo a rede base livre de congestionamentos e atuando apenas como o juiz final das liquidações (POON; DRYJA, 2016; ANTONOPOULOS; HARDING, 2023).

3.7 Pseudonimato e rastreabilidade no Bitcoin

O Bitcoin é frequentemente associado à ideia de anonimato, mas essa interpretação não é tecnicamente precisa. Embora o protocolo não exija, por si só, a identificação civil dos usuários para a criação de endereços, sua arquitetura não foi concebida para oferecer anonimato absoluto. No modelo descrito por Nakamoto (2008), a privacidade do sistema decorre do uso de chaves públicas como pseudônimos e da recomendação de utilizar novos pares de chaves em transações distintas, a fim de dificultar o vínculo entre operações sucessivas. Ainda assim, o próprio autor observa que algum grau de vinculação permanece inevitável, especialmente em transações com múltiplas entradas, nas quais diferentes endereços podem ser associados a um mesmo usuário. Dessa forma, o Bitcoin deve ser

compreendido mais adequadamente como um sistema pseudoanônimo, e não como um sistema verdadeiramente anônimo (NAKAMOTO, 2008).

Essa limitação decorre, em grande medida, da transparência estrutural do *blockchain*. Como o livro-razão é público, todas as transações permanecem registradas e disponíveis para inspeção, o que permite acompanhar fluxos de pagamento, saldos e relações entre endereços ao longo do tempo. Chervinski e Kreutz (2019) destacam que qualquer usuário com acesso aos dados da cadeia pode observar o saldo de determinados endereços, o que já reduz a privacidade dos participantes. Além disso, a reutilização de endereços e o uso de múltiplas entradas em uma mesma transação favorecem heurísticas de agrupamento, permitindo vincular diferentes endereços a um provável controlador comum. Nessa direção, Meiklejohn *et al*. (2013) demonstram que a análise sistemática da *blockchain* permite caracterizar fluxos de pagamento e identificar agrupamentos de entidades, evidenciando que a exposição pública dos dados transacionais cria condições para rastreabilidade e inferência de identidade. (CHERVINSKI; KREUTZ, 2019; MEIKLEJOHN *et al*., 2013).

A fragilidade da privacidade no Bitcoin não se restringe, contudo, à análise *on-chain*. A camada de rede também pode fornecer informações úteis para a desanonimização. Pimentel (2017), ao sintetizar a literatura sobre o tema, aponta que o anonimato das transações pode ser comprometido por técnicas de rastreabilidade cronológica na *blockchain* e pela análise de endereços de rede. Em linha semelhante, Biryukov, Khovratovich e Pustogarov (2014 *apud* PIMENTEL, 2017) mostram que é possível relacionar pseudônimos do Bitcoin aos endereços IP (*Internet Protocol*) a partir dos quais as transações são difundidas na rede P2P. Já Dupont e Squicciarini (2015 *apud* PIMENTEL, 2017) indicam que a correlação entre dados temporais, fusos horários e informações publicamente expostas em fóruns pode contribuir para inferir a localização de usuários. Assim, a quebra de privacidade no ecossistema Bitcoin pode resultar tanto da análise do conteúdo público do *blockchain* quanto da correlação com metadados externos à própria cadeia.

Diante desse cenário, conclui-se que o Bitcoin privilegia a verificabilidade pública, a auditabilidade e a integridade histórica das transações, mas não oferece garantias robustas de anonimato. Sua privacidade depende, em grande parte, do comportamento operacional do usuário, como evitar a reutilização de endereços e reduzir a exposição de metadados que possam ser correlacionados com a atividade *on-chain*. Em outras palavras, a transparência que sustenta a confiança

descentralizada da rede é a mesma característica que permite a realização de análises forenses e mecanismos de rastreabilidade. Por essa razão, o anonimato no Bitcoin deve ser tratado como limitado e condicional, e não como uma propriedade absoluta do protocolo. (NAKAMOTO, 2008; CHERVINSKI; KREUTZ, 2019; PIMENTEL, 2017).

3.8 Síntese do capítulo

A análise da arquitetura do Bitcoin permite compreender que essa rede foi criada com um propósito bem definido: viabilizar a transferência descentralizada de valor sem a necessidade de uma autoridade central. Para isso, sua arquitetura combina elementos criptográficos, estruturais e econômicos que se reforçam mutuamente, resultando em um sistema robusto e previsível, ainda que com limitações intencionais em termos de flexibilidade e escalabilidade.

Ao longo deste capítulo, observou-se que a solução proposta por Nakamoto (2008) para o problema do gasto duplo estabeleceu as bases de toda a arquitetura subsequente. O encadeamento criptográfico dos blocos, o modelo de UTXOs e o mecanismo de Prova de Trabalho formam um conjunto coerente de escolhas de projeto voltadas à segurança e à imutabilidade do registro histórico. A Árvore de *Merkle*, por sua vez, contribui para a eficiência na verificação das transações sem comprometer a integridade do sistema.

Do ponto de vista econômico, a política monetária do Bitcoin se destaca pela previsibilidade. O limite máximo de 21 milhões de unidades e o mecanismo de *halving* conferem ao protocolo uma lógica deflacionária programada e transparente, diferenciando-o estruturalmente dos sistemas monetários tradicionais. Essa característica reforça o papel do Bitcoin como sistema de transferência e reserva de valor descentralizada.

No entanto, a arquitetura do Bitcoin também apresenta limitações relevantes. A capacidade de processamento da camada principal é restrita por *design*, o que impõe desafios de escalabilidade em cenários de alta demanda. A resposta desenvolvida pelo ecossistema foi a criação de soluções de segunda camada, como a *Lightning Network*, que ampliam a capacidade transacional sem alterar o protocolo base. Da mesma forma, a privacidade do Bitcoin é limitada pelo caráter público do livro-razão,

configurando um modelo de pseudonimato sujeito a técnicas de rastreabilidade e análise forense.

Encerrada a análise da arquitetura do Bitcoin, o próximo capítulo examinará a arquitetura do Ethereum, com foco em sua proposta programável e nos elementos que a distinguem estruturalmente da rede apresentada neste capítulo.

4 A ARQUITETURA DO ETHEREUM

O Ethereum surgiu como uma ampliação das possibilidades introduzidas pela tecnologia *blockchain*. Enquanto o Bitcoin se consolidou como a primeira aplicação bem-sucedida de um sistema descentralizado de transferência de valor, o Ethereum foi concebido para oferecer uma infraestrutura mais abrangente, capaz de suportar não apenas transações monetárias, mas também a execução de instruções computacionais por meio de contratos inteligentes. Em sua formulação original, a plataforma foi proposta como uma *blockchain* com linguagem de programação Turing-completa, permitindo a criação de aplicações descentralizadas com finalidades diversas (BUTERIN, 2014).

Sob essa perspectiva, o Ethereum pode ser compreendido como uma generalização do paradigma *blockchain*. Em vez de operar apenas como um livro-razão voltado ao registro de transferências de valor, sua arquitetura foi estruturada como uma máquina de estados baseada em transações, na qual contas e contratos interagem por meio de mensagens e alterações sucessivas no estado global da rede (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

Além disso, a arquitetura do Ethereum passou por transformações relevantes ao longo do tempo. Na formulação contemporânea do protocolo, a rede pode ser compreendida a partir da separação entre camada de execução e camada de consenso, preservando a lógica de computação descentralizada que a distingue de *blockchains* voltadas exclusivamente à transferência de ativos (WOOD, 2025).

Diante disso, este capítulo tem como objetivo analisar os principais elementos que compõem a arquitetura do Ethereum, com destaque para sua origem, sua estrutura de contas, a lógica de transição de estados, a *Ethereum Virtual Machine* (EVM), o mecanismo de cobrança de *gas* e a evolução de seu consenso distribuído. A compreensão desses aspectos é fundamental para, posteriormente, estabelecer uma comparação técnica consistente entre Bitcoin e Ethereum (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

4.1 O surgimento do Ethereum e a expansão da proposta da blockchain

O surgimento do Ethereum está diretamente relacionado às limitações observadas nas primeiras aplicações da tecnologia *blockchain*, especialmente no

Bitcoin. Embora o Bitcoin tenha demonstrado a viabilidade de um sistema descentralizado para registro e transferência de valor, sua arquitetura foi concebida para um propósito relativamente específico. A expansão do uso da *blockchain* para aplicações mais complexas, como ativos digitais, sistemas de reputação, derivativos e contratos inteligentes sofisticados, exigia uma base computacional mais flexível do que aquela disponível no modelo original (BUTERIN, 2014).

Nesse contexto, Vitalik Buterin propôs o Ethereum como uma plataforma capaz de integrar e ampliar ideias que já vinham sendo discutidas no ecossistema das criptomoedas, como *scripts*, metaprotocolos e aplicações descentralizadas. A proposta central era oferecer uma camada fundamental sobre a qual desenvolvedores pudessem construir sistemas com regras próprias de propriedade, transação e transição de estado. Em vez de restringir a *blockchain* a uma função única, o Ethereum foi projetado como um sistema aberto, apto a servir de base a múltiplos protocolos e aplicações (BUTERIN, 2014).

Do ponto de vista conceitual, a diferença fundamental entre Bitcoin e Ethereum está no grau de programabilidade oferecido por cada rede. O Bitcoin introduziu uma inovação decisiva ao resolver o problema do consenso descentralizado em um ambiente aberto, utilizando *blockchain* e prova de trabalho. Contudo, o Ethereum buscou avançar além dessa solução ao propor uma arquitetura em que o *blockchain* deixasse de ser apenas um registro de transações e passasse a funcionar como uma infraestrutura computacional descentralizada, capaz de executar instruções mais complexas e manter estados persistentes entre interações (BUTERIN, 2014; WOOD, 2025).

Essa ampliação da proposta *blockchain* também aparece na forma como o próprio protocolo é definido. No *Yellow Paper*, o Ethereum é descrito como um livro-razão transacional descentralizado generalizado, no qual múltiplos recursos computacionais com estados próprios podem interagir por meio de um mecanismo de troca de mensagens. Em termos práticos, isso significa que a rede não se limita ao envio de unidades monetárias entre usuários, mas permite a execução autônoma de contratos e aplicações distribuídas, com lógica programável e armazenamento persistente (WOOD, 2025).

Desse modo, o Ethereum representa um marco na evolução da *blockchain* ao deslocar o foco da simples movimentação de valor para a construção de uma plataforma programável. Essa característica foi decisiva para o surgimento de um

ecossistema mais amplo de aplicações descentralizadas, incluindo emissão de tokens, finanças descentralizadas, organizações autônomas e diferentes modelos de interação digital baseados em contratos inteligentes (ANTONOPOULOS; WOOD, 2018; BUTERIN, 2014). Assim, compreender o contexto de surgimento do Ethereum é essencial para entender por que sua arquitetura difere substancialmente da arquitetura do Bitcoin e por que essa distinção é central para a análise comparativa proposta neste trabalho.

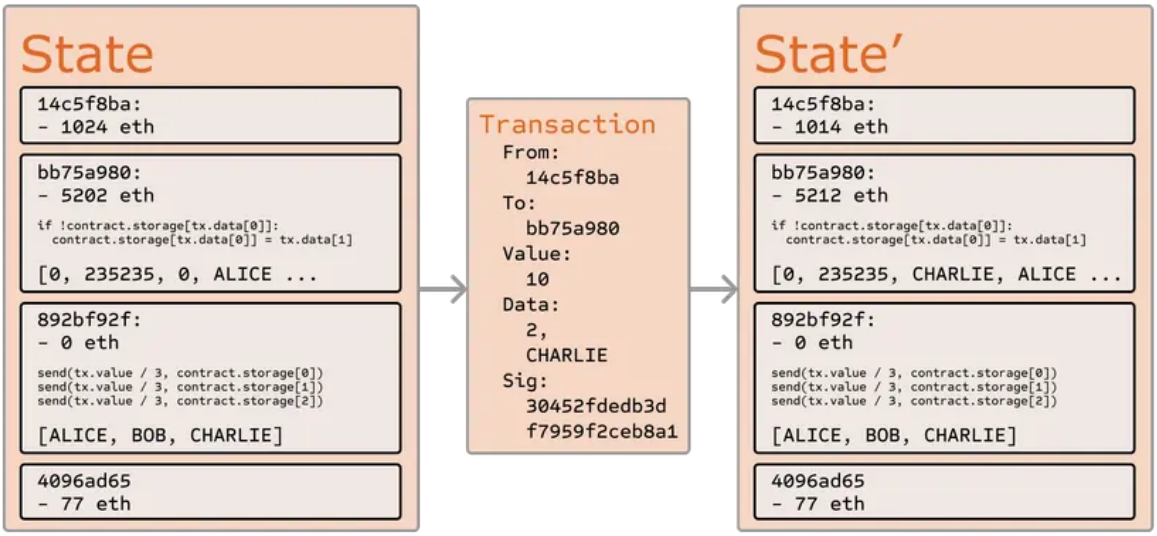
4.2 Blocos, transações e estado global da rede Ethereum

A rede Ethereum pode ser compreendida como uma máquina de estados distribuída. Isso significa que seu funcionamento não se limita ao simples registro de transferências de valor, mas envolve a atualização contínua do estado da rede a partir da execução de transações válidas. Nessa arquitetura, a *blockchain* atua como a base que organiza e valida essas mudanças de forma descentralizada (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

Os blocos do Ethereum reúnem transações válidas e as encadeiam criptograficamente, preservando o histórico das operações realizadas. No entanto, o elemento central da rede não é apenas a sequência de blocos, mas o estado global, isto é, a condição corrente do sistema após a aplicação dessas transações. Assim, os blocos registram o histórico das alterações, enquanto o estado global representa o resultado atual dessas mudanças (WOOD, 2025).

Buterin (2014) explica essa lógica por meio da função de transição de estado, representada por $APPLY(S,TX) \rightarrow S'$, em que uma transação válida, aplicada a um estado anterior, gera um novo estado. Isso demonstra que, no Ethereum, a transação não serve apenas para transferir ether entre contas, mas também para acionar execuções e modificar dados associados à rede.

Figura 10 – Representação da função de transição de estado no Ethereum.



Fonte: Buterin (2014, p. 15).

Como mostra a Figura 10, uma transação altera o estado anterior da rede e produz um novo estado após sua execução. Esse modelo é uma das principais características do Ethereum, pois permite que a *blockchain* suporte não apenas movimentações financeiras, mas também contratos inteligentes e aplicações descentralizadas. Desse modo, a estrutura da rede se organiza pela relação entre blocos, transações e estado global, formando a base arquitetural do protocolo (BUTERIN, 2014; WOOD, 2025).

4.3 O modelo de contas no Ethereum

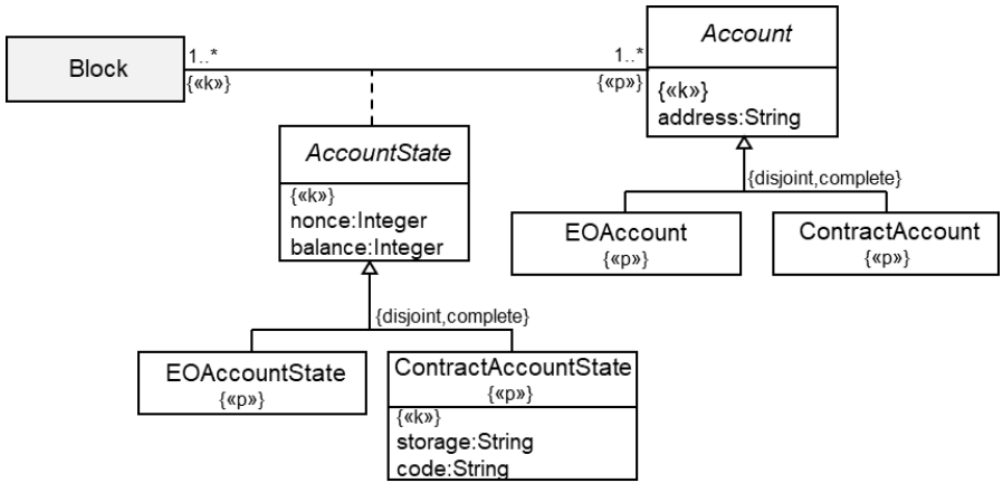
Diferentemente do Bitcoin, que utiliza o modelo de saídas de transações não gastas (*UTXO*), o Ethereum adota um modelo baseado em contas. Nesse sistema, o estado da rede é organizado a partir de contas identificadas por endereços, e as mudanças no sistema ocorrem por meio de transações que alteram o saldo, o código e os dados associados a essas contas. Essa escolha arquitetural é uma das bases que tornam o Ethereum mais adequado à execução de contratos inteligentes e ao suporte de aplicações descentralizadas (BUTERIN, 2014).

De modo geral, uma conta no Ethereum reúne elementos que descrevem seu estado dentro da rede. Entre esses elementos, destacam-se o *nonce*, utilizado para contabilizar transações ou criações associadas à conta, o saldo (*balance*), que representa a quantidade de ether vinculada ao endereço, e, no caso das contas de

contrato, os campos de *armazenamento (storage)* e código (*code*), responsáveis, respectivamente, pelo armazenamento persistente de dados e pelo código executável do contrato. Essa estrutura evidencia que, no Ethereum, a conta não representa apenas um saldo monetário, mas também uma unidade lógica capaz de armazenar informação e comportamento computacional (BUTERIN, 2014; WOOD, 2025).

O protocolo distingue dois tipos principais de contas: as contas externas (*externally owned accounts* – EOAs) e as contas de contrato (*contract accounts*). As contas externas são controladas por quem possui a chave privada correspondente e, por isso, normalmente representam os usuários da rede. Já as contas de contrato são controladas por código e passam a executar funções quando acionadas por transações ou chamadas apropriadas. Em termos práticos, isso significa que as contas externas costumam iniciar operações, enquanto as contas de contrato ampliam as funcionalidades da *blockchain* ao executar lógica programável (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Figura 11 – Contas e seus estados no Ethereum.



Fonte: Olivé (2020, p. 6).

A Figura 11 sintetiza visualmente essa organização. Nela, observa-se que a entidade *Account* se divide em *EOAccount* e *ContractAccount*, correspondendo aos dois tipos de contas existentes no Ethereum. A figura também mostra que toda conta possui um estado associado (*AccountState*), no qual aparecem os atributos *nonce* e *balance*. No caso das contas de contrato, surgem ainda os campos armazenamento

(*storage*) e código (*code*), ligados ao armazenamento persistente de dados e ao código executável do contrato. Dessa forma, a imagem ajuda a compreender que o modelo de contas do Ethereum está diretamente relacionado à manutenção do estado global da rede (OLIVÉ, 2020).

Essa distinção entre contas externas e contas de contrato é central para a arquitetura do Ethereum. Enquanto as contas externas dependem de chaves privadas para enviar transações, as contas de contrato dependem do código que armazenam e executam. Como consequência, o modelo de contas do Ethereum vai além do simples registro de propriedade de ativos, permitindo que a rede sustente aplicações em que dados e funções permanecem disponíveis de forma distribuída. Por essa razão, compreender o modelo de contas é essencial para entender, na próxima seção, o papel da Ethereum Virtual Machine na execução dos contratos inteligentes (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

4.4 Ethereum Virtual Machine (EVM) e contratos inteligentes

A *Ethereum Virtual Machine* (EVM) é o componente responsável pela execução dos contratos inteligentes na rede Ethereum. De forma geral, ela pode ser entendida como um ambiente computacional descentralizado que processa o código dos contratos e atualiza o estado da rede conforme as regras do protocolo. Diferentemente de uma *blockchain* voltada apenas à transferência de valor, o Ethereum incorpora uma camada de execução que permite transformar instruções programáveis em operações válidas dentro do sistema. (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

No whitepaper original, Buterin (2014) explica que o Ethereum foi concebido como uma *blockchain* com linguagem de programação embutida, permitindo que desenvolvedores escrevam contratos inteligentes e aplicações descentralizadas com regras próprias de funcionamento. Nesse contexto, os contratos inteligentes podem ser compreendidos como programas armazenados na *blockchain* que executam automaticamente determinadas instruções quando recebem uma mensagem ou transação apropriada. (BUTERIN, 2014).

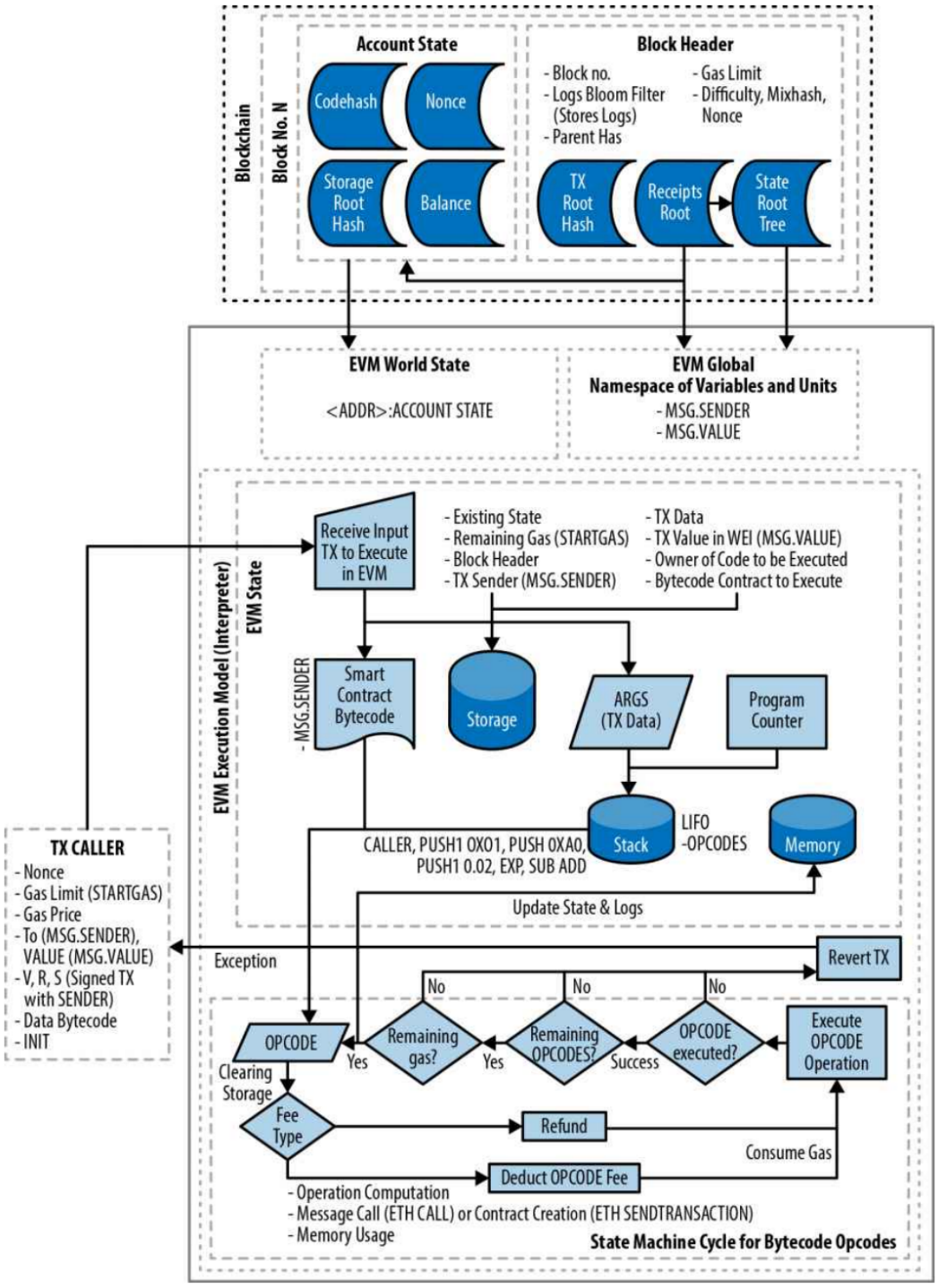
Do ponto de vista técnico, a EVM executa um código de baixo nível conhecido como *EVM bytecode*. Segundo Buterin (2014), esse processo ocorre em uma máquina baseada em pilha, que utiliza pilha (*stack*), memória (*memory*) e armazenamento (*storage*) como espaços distintos para manipulação de dados. Enquanto a memória é

temporária e existe apenas durante a execução, o armazenamento do contrato é persistente e permanece associado à conta de contrato no estado global da rede. (BUTERIN, 2014).

Além disso, a execução dos contratos não ocorre de forma autônoma ou paralela. Conforme destacam Antonopoulos e Wood (2018), um contrato inteligente só é executado quando uma transação iniciada por uma conta externa o aciona diretamente, ou quando outro contrato o chama durante uma cadeia de execução. Isso significa que os contratos permanecem inativos até serem ativados por uma interação válida e que toda execução ocorre de maneira sequencial, como parte da atualização do estado da rede (ANTONOPOULOS; WOOD, 2018).

A organização dos principais componentes da EVM pode ser observada na Figura 12, que sintetiza os elementos responsáveis pela execução do *bytecode* e pela atualização do estado da rede. (ANTONOPOULOS; WOOD, 2018).

Figura 12 – Arquitetura e contexto de execução da Ethereum Virtual Machine.



Fonte: Antonopoulos e Wood (2018, p. 544).

A Figura 12 apresenta, de forma mais detalhada, a arquitetura interna da Ethereum Virtual Machine. Observa-se que a EVM opera a partir do *bytecode* do contrato, armazenado em uma região separada de código, e executa instruções por meio de uma arquitetura baseada em pilha (*stack-based architecture*). Durante esse

processo, a máquina utiliza três espaços principais de dados: a pilha, empregada nas operações imediatas; a memória, que é temporária e existe apenas durante a execução; e o storage, que é persistente e permanece associado ao contrato no estado global da rede. Essa distinção é fundamental porque evidencia que nem toda informação manipulada por um contrato possui a mesma duração ou função dentro do sistema. (ANTONOPOULOS; WOOD, 2018; BUTERIN, 2014).

A figura também evidencia que a execução na EVM depende de um contexto de execução, formado por dados da transação e do bloco, como remetente, valor enviado, dados de entrada e informações do bloco corrente. Além disso, o processamento é acompanhado pelo contador de programa (*program counter* – pc) , que indica a próxima instrução a ser executada, e pela quantidade disponível de *gas*, que limita o número de etapas computacionais possíveis. Dessa forma, a imagem mostra que a EVM não funciona apenas como um interpretador de código, mas como o mecanismo que integra instruções, memória, armazenamento e contexto transacional para produzir atualizações válidas no estado do Ethereum. (BUTERIN, 2014; WOOD, 2025).

Outro aspecto relevante é que a execução na EVM é limitada por *gas*, o que impede laços infinitos e consumo ilimitado de recursos computacionais. Por isso, embora o Ethereum ofereça uma linguagem programável com grande flexibilidade, sua máquina virtual opera dentro de limites bem definidos, preservando a viabilidade do protocolo. Assim, a EVM constitui a base que torna possível a existência de contratos inteligentes, aplicações descentralizadas e outros serviços programáveis sobre a *blockchain* do Ethereum. (ANTONOPOULOS; WOOD, 2018; BUTERIN, 2014).

4.5 Gas, taxas e custo computacional

No Ethereum, a execução de operações computacionais não ocorre de forma gratuita. Para evitar abuso da rede e limitar o consumo excessivo de recursos, o protocolo adota o mecanismo de *gas*, que funciona como uma unidade de medida do custo computacional e de armazenamento exigido por transações e contratos inteligentes. Dessa forma, cada operação executada na EVM possui um custo previamente definido, o que permite controlar a utilização da infraestrutura

descentralizada e reduzir riscos como *spam* e *loops* infinitos (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

Nesse modelo, é importante distinguir *custo de gas (gas cost)* de preço do gas (*gas price*). O primeiro corresponde à quantidade de unidades de *gas* necessária para executar determinada operação, enquanto o segundo representa o valor pago por cada unidade de *gas*. Assim, o custo total de uma transação depende tanto da complexidade computacional da execução quanto do preço que o usuário está disposto a pagar para que sua transação seja processada. Em termos práticos, essa separação permite que o Ethereum mensure computação de forma independente da cotação do ether no mercado (ANTONOPOULOS; WOOD, 2018).

Além disso, toda transação define um *limite de gas (gas limit)*, isto é, um limite máximo de *gas* que poderá ser consumido durante sua execução. Se a execução terminar antes de atingir esse limite, o valor correspondente ao *gas* não utilizado é reembolsado ao remetente. Por outro lado, se a transação consumir todo o *gas* disponível, ocorre a condição conhecida como *esgotamento de gas (out of gas)*, interrompendo a execução e revertendo as alterações de estado produzidas até aquele ponto. Ainda assim, o custo computacional já realizado precisa ser pago, uma vez que a rede já empregou recursos para processar a operação (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

Na formulação mais recente do protocolo, o mecanismo de taxas também passou a incorporar a lógica introduzida pela EIP-1559 (Ethereum Improvement Proposal 1559). De acordo com o *Yellow Paper*, cada transação incluída em bloco deve pagar uma *base fee,* expressa em *wei* por unidade de *gas* consumido, que é queimada da circulação. Além disso, pode haver uma *priority fee*, destinada ao validador responsável pela inclusão da transação. Essa estrutura busca tornar a precificação mais previsível e ajustar dinamicamente a taxa básica de acordo com a demanda por espaço em bloco (WOOD, 2025).

Desse modo, o mecanismo de *gas* exerce papel central na arquitetura do Ethereum, pois conecta execução computacional, segurança e incentivo econômico. Mais do que uma simples taxa de transação, o *gas* funciona como um instrumento de regulação interna da rede, limitando o custo das operações, remunerando a validação e preservando a viabilidade do protocolo diante da execução de contratos inteligentes e aplicações descentralizadas (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

4.6 A transição do Ethereum da Proof-of-Work para a Proof-of-Stake

O mecanismo de consenso é o conjunto de regras que permite à rede decidir quais blocos e transações passam a fazer parte da história válida do sistema. Em outras palavras, é ele que garante que os participantes da rede reconheçam uma mesma sequência de atualizações como a versão correta da *blockchain*. No caso do Ethereum, esse mecanismo passou por uma mudança profunda ao longo do tempo, saindo de um modelo baseado em mineração para outro baseado em validação por depósito de criptomoeda (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

Na fase inicial do Ethereum, o consenso era realizado por *PoW*. Nesse modelo, os mineradores competiam para resolver um problema computacional e, ao encontrar uma solução válida, ganhavam o direito de propor um novo bloco. Como explicam Antonopoulos e Wood (2018), o objetivo principal desse processo não era apenas criar novas unidades de ether, mas proteger a rede de forma descentralizada. O custo com energia e infraestrutura funcionava como um desincentivo econômico para comportamentos desonestos.

No Ethereum, esse modelo utilizava o algoritmo *Ethash*, desenvolvido para depender do acesso a uma grande estrutura de dados e, assim, reduzir a vantagem de equipamentos excessivamente especializados. A intenção era dificultar a concentração da mineração em poucos agentes. Mesmo assim, desde cedo já existia no projeto a expectativa de substituir esse modelo. O próprio *Mastering Ethereum* destaca que a chamada *difficulty bomb* foi criada justamente para tornar a mineração progressivamente menos viável e pressionar a transição para PoS (ANTONOPOULOS; WOOD, 2018).

No modelo de PoS, a segurança da rede deixa de depender de mineradores e passa a depender de validadores. Nesse sistema, quem deseja participar do consenso precisa bloquear uma quantidade de ether como depósito. A rede então seleciona validadores para propor e confirmar blocos, e o peso da participação está ligado ao valor colocado em *stake*. A principal diferença econômica em relação ao PoW é que, no PoS, a punição por comportamento inadequado ocorre dentro do próprio protocolo, por meio do risco de perda do valor depositado, e não por gasto externo com eletricidade e hardware (ANTONOPOULOS; WOOD, 2018).

Outra consequência importante dessa mudança foi a separação entre camada de execução e camada de consenso. O *Yellow Paper* atual deixa claro que a *Beacon*

Chain passou a definir a história canônica dos blocos, enquanto a camada de execução continua responsável pelas regras de atualização do estado da máquina virtual do Ethereum. O documento também registra que, após essa transição, a rede passou a operar com *slots* de 12 segundos, o que mostra que não se tratou apenas de trocar mineradores por validadores, mas de reorganizar parte relevante da arquitetura do protocolo (WOOD, 2025).

Desse modo, a passagem de PoW para PoS representa uma das mudanças mais importantes da história do Ethereum. Mais do que alterar a forma de criação dos blocos, essa transição modificou a lógica de segurança, os incentivos econômicos e a própria estrutura de coordenação da rede. Por isso, compreender essa evolução é essencial para a comparação com o Bitcoin, que permanece baseado em PoW (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

4.7 Escalabilidade no Ethereum

Escalabilidade é a habilidade de uma rede lidar com um grande número de transações sem comprometer o desempenho ou aumentar os custos de forma excessiva. No caso do Ethereum, esse é um desafio importante porque a rede principal precisa conciliar três objetivos ao mesmo tempo: segurança, descentralização e capacidade de processamento. Como consequência, a camada principal não consegue ampliar indefinidamente o número de transações por segundo, o que pode gerar lentidão e encarecimento do uso da rede em momentos de maior demanda (ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026b).

Para enfrentar esse problema, a estratégia adotada no ecossistema Ethereum passou a priorizar as chamadas soluções de segunda camada, também conhecidas como *Layer* 2. Em vez de executar todas as operações diretamente na rede principal, essas soluções processam parte das transações fora dela e depois enviam ao Ethereum os dados necessários para registro e verificação. Assim, a rede principal continua funcionando como base de segurança, enquanto parte da execução é deslocada para camadas complementares, reduzindo congestionamento e custo para os usuários (ETHEREUM.ORG, 2025b).

Entre essas soluções, destacam-se os *rollups*, que hoje ocupam posição central na estratégia de escalabilidade do Ethereum. Em termos gerais, os *rollups* agrupam muitas transações realizadas fora da rede principal e publicam no Ethereum

um conjunto resumido de dados, preservando a possibilidade de verificação. Há dois grupos principais. Nos *rollups* otimistas (*optimistic rollups*), as transações são consideradas válidas inicialmente e podem ser contestadas depois, caso haja fraude. Já nos *rollups* de conhecimento zero *(zero-knowledge rollups* ou *ZK-rollups),* a validade das operações é demonstrada por meio de provas criptográficas. Apesar das diferenças técnicas, ambos reduzem a carga sobre a rede principal e ampliam sua capacidade prática de uso (ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026a; ETHEREUM.ORG, 2026c).

Além das soluções de segunda camada, o Ethereum também vem recebendo mudanças na própria infraestrutura para tornar esse modelo mais eficiente. Um passo importante foi a atualização *Dencun*, ativada em março de 2024, que introduziu o *Proto-Danksharding* (EIP-4844). Essa mudança criou os chamados *blobs* de dados, um formato mais barato para que os *rollups* publiquem informações na rede. Em termos práticos, isso reduz o custo de armazenamento temporário dos dados necessários para essas soluções e melhora a eficiência da escalabilidade baseada em segunda camada (ETHEREUM.ORG, 2025a).

Desse modo, a escalabilidade do Ethereum não depende apenas do aumento da capacidade da *blockchain* principal, mas de uma arquitetura em múltiplas camadas. A rede principal permanece responsável pela segurança e pela validação fundamental, enquanto as soluções complementares absorvem parte relevante da execução das transações. Isso mostra que o Ethereum passou a seguir uma lógica de expansão baseada na cooperação entre camadas, e não apenas no crescimento direto da capacidade da própria rede principal (ETHEREUM.ORG, 2025a; ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026b).

4.8 Transparência, privacidade e aplicações do Ethereum

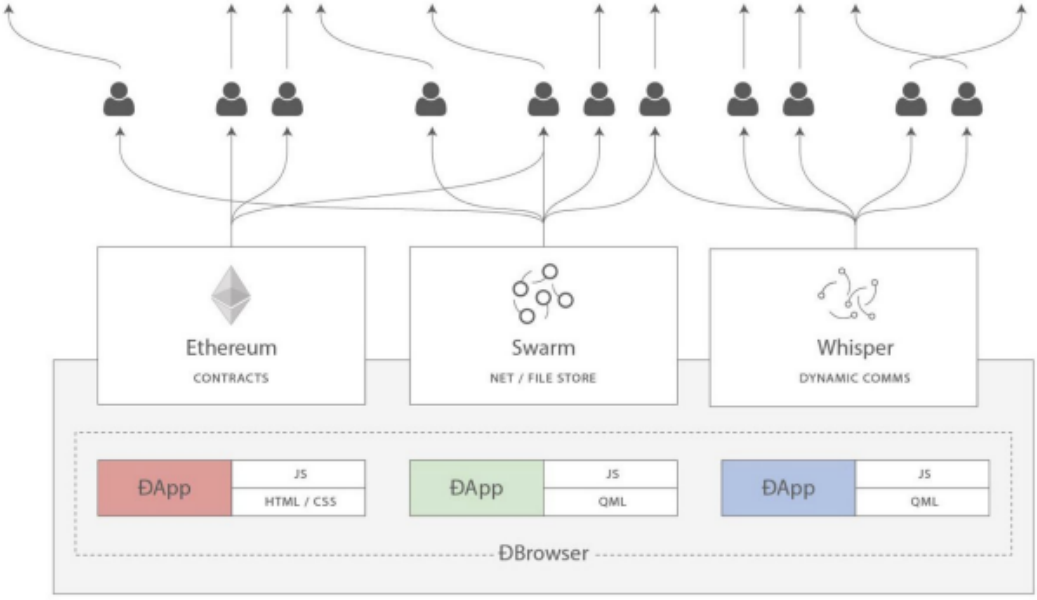
Uma das características mais importantes do Ethereum é sua transparência. Como a rede funciona sobre uma *blockchain* pública, as transações e as interações com contratos inteligentes podem ser registradas e verificadas por qualquer participante. Isso significa que o Ethereum não oferece apenas um meio de transferir valor, mas também um ambiente em que regras, execuções e mudanças de estado podem ser acompanhadas de forma auditável. Essa transparência é uma das bases

da confiança distribuída no protocolo (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

Por outro lado, essa mesma transparência traz limitações em relação à privacidade. Embora os usuários sejam identificados por endereços e não, necessariamente, por nomes civis, as operações permanecem registradas de forma permanente e pública. Assim, o Ethereum não foi projetado para garantir sigilo completo, mas para priorizar verificabilidade e rastreabilidade. Em outras palavras, a rede favorece a confiança no registro das operações, mas não possui a privacidade forte como característica nativa de sua arquitetura (ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

Além disso, o Ethereum se destaca por permitir muito mais do que simples transferências de criptomoeda. Sua arquitetura foi desenvolvida para sustentar contratos inteligentes e aplicações descentralizadas, conhecidas como *DApps (decentralized applications).* Nesse contexto, os contratos inteligentes funcionam como programas executados na *blockchain*, enquanto as *DApps* utilizam esses contratos como base para oferecer serviços digitais sem depender totalmente de um servidor ou intermediário centralizado. Essa característica amplia significativamente o uso da *blockchain* para além do campo financeiro (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Figura 13 – Web3: estrutura de uma web descentralizada baseada em contratos inteligentes e tecnologias P2P.



Fonte: Antonopoulos e Wood (2018, p. 495).

A Figura 13 ajuda a compreender essa ampliação do papel do Ethereum. Em vez de representar a rede apenas como um sistema de pagamentos, a imagem mostra sua inserção em uma estrutura mais ampla de web descentralizada, na qual contratos inteligentes se articulam com tecnologias ponto a ponto para sustentar aplicações digitais. Isso reforça a ideia de que o Ethereum funciona como uma infraestrutura programável, capaz de apoiar diferentes serviços com maior transparência, resistência à censura e menor dependência de intermediários (ANTONOPOULOS; WOOD, 2018).

Na prática, essa arquitetura permite o desenvolvimento de diversas aplicações. O trabalho de Akiau (2023), por exemplo, mostra que contratos inteligentes podem ser usados em plataformas de financiamento coletivo para aumentar a transparência na gestão dos recursos e ampliar o controle dos participantes sobre as regras de execução. De forma mais ampla, o ecossistema Ethereum passou a servir de base para emissão de *tokens*, finanças descentralizadas, sistemas de governança e outros serviços digitais baseados em execução automática de regras. Isso explica por que o Ethereum se consolidou como uma das principais plataformas do universo *blockchain* (AKIAU, 2023; ANTONOPOULOS; WOOD, 2018).

4.9 Síntese do capítulo

A análise da arquitetura do Ethereum permite compreender que essa plataforma representa uma ampliação significativa das possibilidades introduzidas pela *blockchain*. Enquanto o Bitcoin foi estruturado principalmente para viabilizar a transferência descentralizada de valor, o Ethereum foi concebido como uma infraestrutura programável, capaz de executar contratos inteligentes e sustentar aplicações descentralizadas em uma rede pública. Essa diferença de propósito explica por que o Ethereum desenvolveu uma arquitetura mais voltada à computação distribuída e à manutenção de um estado global continuamente atualizado (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Ao longo deste capítulo, observou-se que a estrutura do Ethereum está apoiada em elementos centrais como o modelo de contas, a *Ethereum Virtual Machine*, o mecanismo de *gas* e a lógica de transição de estados. Em conjunto, esses componentes permitem que a rede não apenas registre operações financeiras, mas também processe instruções, armazene dados persistentes e execute regras programáveis de maneira descentralizada. Dessa forma, a *blockchain* do Ethereum assume papel mais amplo do que o de um simples livro-razão transacional, aproximando-se de uma plataforma geral de execução distribuída (BUTERIN, 2014; WOOD, 2025).

Também foi possível verificar que a evolução do Ethereum não se limitou à sua formulação original. A transição de PoW para PoS, bem como a separação entre camada de execução e camada de consenso, demonstram que a rede passou por transformações relevantes em busca de maior eficiência e adaptação às demandas de escalabilidade. Do mesmo modo, a adoção crescente de soluções de segunda camada evidencia que a arquitetura do Ethereum continua em desenvolvimento, preservando sua proposta de programabilidade sem abandonar os requisitos de segurança e descentralização (WOOD, 2025).

Por fim, a combinação entre transparência, execução programável e diversidade de aplicações consolidou o Ethereum como uma das principais infraestruturas do ecossistema *blockchain*. Essa posição decorre de sua capacidade de integrar ativos digitais, contratos inteligentes e aplicações descentralizadas em uma mesma plataforma (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Encerrada a análise da arquitetura do Ethereum, o próximo capítulo apresentará uma comparação direta com o Bitcoin, com o objetivo de identificar convergências, diferenças estruturais e implicações práticas entre as duas redes.

5 ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM

Após a análise individual das arquiteturas do Bitcoin e do Ethereum, desenvolvida nos capítulos anteriores, torna-se possível avançar para uma comparação direta entre essas duas redes. O Capítulo 3 demonstrou que o Bitcoin foi estruturado como um sistema descentralizado de transferência de valor, com ênfase em segurança, previsibilidade e uma política monetária programada. O Capítulo 4, por sua vez, evidenciou que o Ethereum ampliou a proposta da *blockchain* ao incorporar uma arquitetura programável capaz de executar contratos inteligentes e sustentar aplicações descentralizadas. Com essa base construída, este capítulo tem como objetivo estabelecer uma comparação técnica sistemática entre as duas plataformas, a partir de critérios que permitam evidenciar convergências, divergências e implicações práticas de suas escolhas de projeto.

5.1 Critérios e objetivos da análise comparativa

A comparação entre Bitcoin e Ethereum exige considerar que ambas as redes compartilham fundamentos comuns da tecnologia *blockchain*, como descentralização, uso de criptografia e validação distribuída, mas foram concebidas para atender a propósitos distintos. Enquanto o Bitcoin foi proposto como um sistema de dinheiro eletrônico ponto a ponto, com foco na transferência descentralizada de valor, o Ethereum ampliou essa proposta ao incorporar uma infraestrutura programável voltada à execução de contratos inteligentes e aplicações descentralizadas (NAKAMOTO, 2008; BUTERIN, 2014).

Nesse contexto, a análise comparativa entre essas duas redes não deve ser conduzida em termos absolutos de superioridade, mas sim a partir da compreensão de suas diferentes escolhas de projeto. Como observam Lucena e Henriques (2016), Bitcoin e Ethereum apresentam arquiteturas distintas, especialmente no que se refere ao modelo transacional, à lógica de execução e às finalidades atribuídas à *blockchain*. Assim, comparar essas redes significa examinar como cada uma organiza seus mecanismos técnicos para responder a objetivos específicos dentro do ecossistema *blockchain* (LUCENA; HENRIQUES, 2016).

Dessa forma, o objetivo deste capítulo é analisar comparativamente Bitcoin e Ethereum a partir de critérios técnicos centrais, de modo a evidenciar convergências,

divergências e implicações práticas decorrentes de suas arquiteturas. Para isso, a comparação será organizada com base em aspectos como filosofia de design, gestão de estado e modelos transacionais, mecanismos de consenso e segurança, escalabilidade, privacidade, auditabilidade e espectro de aplicações. A partir desses eixos, busca-se construir uma visão comparativa que permita compreender não qual rede é “melhor” de forma universal, mas em que medida suas diferenças refletem propostas e capacidades distintas.

5.2 Filosofia de design e arquitetura de rede

A diferença mais fundamental entre Bitcoin e Ethereum está na filosofia de design que orientou a criação de cada rede. O Bitcoin foi concebido como um sistema de dinheiro eletrônico ponto a ponto, com o objetivo de permitir transações descentralizadas sem a necessidade de intermediários financeiros. Sua arquitetura foi desenvolvida para priorizar segurança, previsibilidade e resistência à censura, mantendo escopo funcional mais restrito e uma linguagem de *script* intencionalmente limitada. Já o Ethereum surgiu com a proposta de ampliar as possibilidades da *blockchain*, oferecendo uma infraestrutura programável capaz de executar contratos inteligentes e sustentar aplicações descentralizadas (NAKAMOTO, 2008; BUTERIN, 2014).

Essa diferença de propósito influencia diretamente a arquitetura de cada rede. No Bitcoin, a *blockchain* funciona principalmente como um livro-razão distribuído voltado ao registro e à validação de transferências de valor. Sua estrutura prioriza a integridade do histórico das transações e a proteção contra o gasto duplo, com menor ênfase em flexibilidade computacional. No Ethereum, por sua vez, a *blockchain* assume papel mais amplo, pois, além de registrar operações, mantém um estado global continuamente atualizado, no qual contas e contratos interagem por meio de regras programáveis. Assim, enquanto o Bitcoin se concentra na confiabilidade do registro monetário, o Ethereum se organiza como uma plataforma de execução distribuída (NAKAMOTO, 2008; WOOD, 2025; BUTERIN, 2014).

Essa distinção também pode ser percebida na forma como cada rede trata a programabilidade. O Bitcoin utiliza uma linguagem de *script* não Turing-completa, o que limita a complexidade das instruções que podem ser executadas diretamente na *blockchain*. Essa limitação é proposital e está associada à busca por maior

previsibilidade e segurança no processamento das transações. Já o Ethereum foi concebido para operar com uma máquina virtual própria, a *Ethereum Virtual Machine*, permitindo a execução de contratos inteligentes com lógica mais sofisticada e armazenamento persistente de dados. Dessa forma, o Ethereum amplia a capacidade funcional da *blockchain*, ao passo que o Bitcoin preserva uma arquitetura mais enxuta e especializada (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Sob a perspectiva do design, pode-se afirmar que o Bitcoin adota uma abordagem mais conservadora, centrada na robustez de um sistema monetário descentralizado, enquanto o Ethereum assume uma proposta mais expansiva, voltada à criação de uma base programável para diferentes tipos de aplicação. Isso não significa que uma rede seja superior à outra em termos absolutos, mas que cada uma foi construída para atender prioridades distintas. Em consequência, a arquitetura do Bitcoin tende a favorecer simplicidade e estabilidade, ao passo que a arquitetura do Ethereum favorece flexibilidade e amplitude de uso (LUCENA; HENRIQUES, 2016; BUTERIN, 2014).

Essa diferença de filosofia de design é decisiva para compreender as demais comparações desenvolvidas neste capítulo. As distinções entre modelo transacional, mecanismo de consenso, escalabilidade e espectro de aplicações decorrem, em grande medida, dessa escolha inicial entre uma *blockchain* voltada prioritariamente à transferência de valor e outra concebida como infraestrutura programável. Por isso, a comparação entre Bitcoin e Ethereum deve partir do reconhecimento de que suas arquiteturas refletem finalidades distintas dentro do ecossistema *blockchain* (LUCENA; HENRIQUES, 2016; NAKAMOTO, 2008; BUTERIN, 2014).

5.3 Gestão de estado nos modelos UTXO e de contas

Uma das diferenças estruturais mais importantes entre Bitcoin e Ethereum está na forma como cada rede organiza e atualiza seu estado interno. No Bitcoin, o modelo adotado é o de saídas de transações não gastas (UTXOs), no qual o saldo de um usuário não é armazenado como um valor único associado a uma conta, mas como um conjunto de saídas disponíveis para gasto em transações futuras. Já no Ethereum, a rede utiliza um modelo de contas, em que cada endereço possui um estado próprio, com saldo, informações de controle e, no caso dos contratos, código e armazenamento persistente. Essa diferença influencia diretamente a forma como as

transações são construídas, verificadas e interpretadas em cada plataforma (NAKAMOTO, 2008; BUTERIN, 2014; WOOD, 2025).

No modelo UTXO do Bitcoin, cada transação consome saídas anteriores como entrada e gera novas saídas que poderão ser utilizadas posteriormente. Isso significa que o sistema não rastreia diretamente um saldo contínuo por endereço, mas sim a disponibilidade de unidades específicas de valor ainda não gastas. Esse arranjo favorece auditabilidade e simplicidade na verificação das transações, além de contribuir para a prevenção do gasto duplo. Em contrapartida, ele também impõe limitações à manipulação de estados mais complexos, uma vez que a lógica transacional está centrada na movimentação e recomposição dessas saídas de valor (NAKAMOTO, 2008; ANTONOPOULOS; HARDING, 2023).

No Ethereum, o funcionamento é distinto. A rede mantém um estado global composto por contas identificadas por endereços, e cada conta possui elementos que descrevem sua condição atual. No caso das contas externas, esse estado inclui principalmente *nonce* e saldo; no caso das contas de contrato, inclui também código executável e armazenamento persistente. Nesse modelo, as transações provocam alterações diretas nesse estado, sem a necessidade de consumir e recriar unidades discretas de valor, como ocorre no Bitcoin. Isso torna a atualização do sistema mais adequada a aplicações que dependem de memória persistente, interação entre contratos e execução contínua de regras programáveis (BUTERIN, 2014; WOOD, 2025).

Do ponto de vista comparativo, o modelo UTXO tende a oferecer uma estrutura mais enxuta e especializada para transferência de valor, ao passo que o modelo de contas favorece maior flexibilidade para aplicações computacionais. No Bitcoin, a lógica de entradas e saídas se ajusta bem à proposta de um sistema monetário descentralizado, em que a prioridade está na segurança e na rastreabilidade das transferências. No Ethereum, por outro lado, a presença de contas com estado persistente cria as condições necessárias para o funcionamento de contratos inteligentes e aplicações descentralizadas mais complexas. Assim, a diferença entre UTXO e modelo de contas não é apenas operacional, mas reflete escolhas arquiteturais compatíveis com os propósitos centrais de cada rede (LUCENA; HENRIQUES, 2016; BUTERIN, 2014).

Além disso, essa distinção produz efeitos importantes na experiência de uso e na forma de desenvolver aplicações sobre cada *blockchain*. No Bitcoin, a composição

de transações com múltiplas entradas e saídas, inclusive para geração de troco, decorre diretamente da lógica do modelo UTXO. No Ethereum, a atualização de saldos e estados ocorre de forma mais próxima à ideia tradicional de contas, o que tende a simplificar determinadas operações e facilitar a construção de aplicações com lógica de negócio persistente. Em consequência, a comparação entre esses dois modelos evidencia que Bitcoin e Ethereum não apenas executam transações de maneiras diferentes, mas organizam o próprio funcionamento interno da rede a partir de concepções distintas de estado e valor (ANTONOPOULOS; HARDING, 2023; ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

5.4 Consenso e segurança no Proof-of-Work e no Proof-of-Stake

Os mecanismos de consenso adotados por Bitcoin e Ethereum revelam uma diferença central entre as duas redes, tanto do ponto de vista técnico quanto econômico. O Bitcoin permanece baseado na prova de trabalho, em que mineradores competem para resolver problemas computacionais e, assim, obter o direito de adicionar novos blocos à *blockchain*. Já o Ethereum, após operar inicialmente com esse mesmo modelo, passou a utilizar a prova de participação, na qual validadores são selecionados com base no valor bloqueado em stake. Em ambos os casos, o objetivo é assegurar a integridade do histórico da rede e evitar comportamentos maliciosos, mas os meios utilizados para isso são bastante distintos (NAKAMOTO, 2008; WOOD, 2025).

No Bitcoin, a segurança está associada ao elevado custo externo exigido pela mineração. Para propor um bloco válido, os mineradores precisam investir em poder computacional e consumo de energia, o que torna economicamente caro tentar reescrever a cadeia ou atacar a rede. Esse modelo confere ao Bitcoin alto grau de robustez, pois a proteção do sistema depende de recursos físicos e financeiros mobilizados fora do próprio protocolo. Ao mesmo tempo, essa característica também faz com que a rede seja frequentemente associada a alto gasto energético, uma vez que o processo de consenso exige competição contínua entre os participantes da mineração (NAKAMOTO, 2008; ANTONOPOULOS; HARDING, 2023).

No Ethereum, a lógica de segurança foi reformulada com a adoção do PoS. Em vez de competir por meio de força computacional, os participantes da validação precisam bloquear uma quantidade de ether como depósito para atuar como

validadores. Nesse modelo, a segurança deixa de depender do gasto externo com eletricidade e *hardware* e passa a se basear em incentivos internos ao protocolo. Caso um validador se comporte de forma inadequada, parte do valor depositado pode ser perdida, o que funciona como mecanismo de punição econômica. Assim, a proteção da rede se apoia menos em capacidade computacional e mais em comprometimento de capital dentro do próprio sistema (WOOD, 2025; ANTONOPOULOS; WOOD, 2018).

Essa diferença também produz efeitos relevantes sobre o funcionamento das redes. No Bitcoin, o consenso por PoW está diretamente ligado à mineração e à emissão de novos bitcoins, de modo que a criação de blocos, a segurança da rede e a política monetária se articulam de forma estreita. No Ethereum, após a transição para PoS, a camada de consenso passou a operar por meio da *Beacon Chain*, enquanto a camada de execução permaneceu responsável pelo processamento das transações e pela atualização do estado da rede. Com isso, o Ethereum passou a apresentar uma separação mais clara entre validação e execução, o que representa uma mudança arquitetural importante em relação ao modelo tradicional de *blockchain* baseado em mineração (WOOD, 2025).

Do ponto de vista comparativo, pode-se afirmar que o Bitcoin privilegia um modelo de segurança fundamentado em custo energético e trabalho computacional, enquanto o Ethereum adota um modelo fundamentado em participação econômica e risco de perda do capital bloqueado. O primeiro tende a reforçar a ideia de segurança vinculada a recursos físicos externos ao protocolo; o segundo busca reduzir custos energéticos e reorganizar os incentivos dentro da própria rede. Dessa forma, a comparação entre PoW e PoS evidencia não apenas duas soluções distintas para o problema do consenso distribuído, mas também duas concepções diferentes de como sustentar a segurança de uma *blockchain* pública (NAKAMOTO, 2008; WOOD, 2025; GRANDJEAN; HEIMBACH; WATTENHOFER, 2023).

5.5 Escalabilidade e soluções de segunda camada

A escalabilidade constitui um desafio relevante tanto para o Bitcoin quanto para o Ethereum, embora cada rede enfrente esse problema de forma distinta. Em ambos

os casos, a camada principal da *blockchain* foi projetada para priorizar segurança e descentralização, o que limita a quantidade de transações que pode ser processada diretamente na rede base. Como consequência, em períodos de maior demanda, podem ocorrer congestionamento, aumento das taxas e redução da eficiência operacional (ANTONOPOULOS; HARDING, 2023; ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026b).

No Bitcoin, essa limitação decorre principalmente do tamanho dos blocos, do intervalo médio de geração e da própria opção de manter uma camada base mais conservadora. Essa escolha favorece robustez e previsibilidade, mas reduz a capacidade de processamento direto da rede. Para lidar com esse cenário, foram desenvolvidas soluções de segunda camada, com destaque para a *Lightning Network*, que permite a realização de múltiplas transações fora da *blockchain* principal, registrando na cadeia base apenas a abertura e o encerramento dos canais de pagamento. Dessa forma, busca-se ampliar a capacidade prática de uso do Bitcoin sem alterar profundamente a estrutura de sua camada principal (ANTONOPOULOS; HARDING, 2023).

No Ethereum, o problema da escalabilidade também se manifesta na camada principal, especialmente pelo fato de a rede não se limitar à transferência de valor, mas também executar contratos inteligentes e aplicações descentralizadas. Isso torna a demanda computacional da rede mais ampla e, em muitos momentos, mais intensa. Para enfrentar esse desafio, a estratégia de escalabilidade do Ethereum passou a se apoiar fortemente em soluções de segunda camada, especialmente os *rollups*, que processam transações fora da rede principal e depois publicam no Ethereum os dados necessários para validação e segurança (ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026b).

Entre essas soluções, destacam-se os *rollups* otimistas e os rollups de conhecimento zero. Nos primeiros, as transações são inicialmente consideradas válidas e podem ser contestadas posteriormente em caso de fraude. Nos segundos, a validade das operações é demonstrada por meio de provas criptográficas. Embora adotem mecanismos diferentes, ambas as abordagens buscam reduzir a carga sobre a camada principal e diminuir o custo de uso da rede. Além disso, atualizações recentes do Ethereum, como a introdução de novos mecanismos de disponibilidade de dados, reforçam essa estratégia de escalabilidade baseada na cooperação entre a

camada principal e soluções complementares (ETHEREUM.ORG, 2025a; ETHEREUM.ORG, 2026a; ETHEREUM.ORG, 2026c).

Do ponto de vista comparativo, observa-se que Bitcoin e Ethereum enfrentam limitações semelhantes na camada base, mas adotam respostas diferentes de acordo com suas prioridades arquiteturais. No Bitcoin, a solução de segunda camada é fortemente orientada para pagamentos mais rápidos e baratos, preservando a simplicidade da *blockchain* principal. No Ethereum, as soluções de segunda camada assumem papel mais amplo, buscando sustentar não apenas transações monetárias, mas também a execução de aplicações descentralizadas em um ecossistema programável. Assim, a comparação evidencia que a escalabilidade, em ambos os casos, deixou de depender apenas da expansão da camada principal e passou a ser tratada por meio de arquiteturas complementares (ANTONOPOULOS; HARDING, 2023; ETHEREUM.ORG, 2025b; ETHEREUM.ORG, 2026b).

5.6 Privacidade, auditabilidade e espectro de aplicações

Bitcoin e Ethereum compartilham uma característica fundamental: ambas são redes públicas, nas quais as transações e os registros podem ser verificados pelos participantes. Essa transparência contribui para a auditabilidade das operações e para a confiança distribuída no sistema, uma vez que o histórico da *blockchain* permanece acessível e verificável. No entanto, essa mesma característica também impõe limites à privacidade, pois as interações realizadas na rede podem ser rastreadas e analisadas, ainda que os usuários não sejam identificados diretamente por nomes civis (ANTONOPOULOS; HARDING, 2023; ANTONOPOULOS; WOOD, 2018).

No Bitcoin, a privacidade é normalmente descrita como pseudonimato. Isso significa que as transações são associadas a endereços criptográficos, e não diretamente à identidade real do usuário. Apesar disso, como o histórico das operações é público, a análise do fluxo de transações pode permitir a identificação de padrões e, em alguns casos, a vinculação entre endereços e indivíduos. Assim, o Bitcoin não oferece anonimato pleno, mas sim um modelo de privacidade limitado, no qual a transparência do livro-razão se mantém como característica central da rede (ANTONOPOULOS; HARDING, 2023).

No Ethereum, a situação é semelhante em relação à visibilidade das operações, mas a presença de contratos inteligentes e aplicações descentralizadas

amplia o escopo do que pode ser observado na *blockchain*. Além das transferências de ether, a rede registra interações com contratos, mudanças de estado e execuções de lógica programável, o que torna a auditabilidade ainda mais abrangente. Em contrapartida, isso também significa que a exposição pública não se restringe ao fluxo monetário, alcançando dados e comportamentos associados ao funcionamento das aplicações descentralizadas (BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018; WOOD, 2025).

A principal diferença entre as duas redes, entretanto, aparece de forma mais clara no espectro de aplicações. O Bitcoin foi concebido primordialmente como um sistema descentralizado de transferência de valor e, ao longo do tempo, consolidou-se sobretudo como ativo digital associado a reserva de valor e resistência à censura. Já o Ethereum foi projetado como uma infraestrutura programável, capaz de sustentar contratos inteligentes e aplicações descentralizadas em diferentes contextos. Essa característica permitiu a expansão de seu ecossistema para áreas como finanças descentralizadas, emissão de *tokens*, governança digital e outras formas de automação baseada em *blockchain* (NAKAMOTO, 2008; BUTERIN, 2014; ANTONOPOULOS; WOOD, 2018).

Desse modo, a comparação entre Bitcoin e Ethereum mostra que ambas as redes combinam transparência com limitações de privacidade, mas diferem significativamente quanto ao alcance funcional de suas arquiteturas. No Bitcoin, a *blockchain* está mais diretamente associada ao registro e à transferência de valor. No Ethereum, a mesma base tecnológica é ampliada para incluir lógica programável, contratos inteligentes e uma variedade maior de aplicações. Assim, enquanto o Bitcoin se destaca por sua especialização como sistema monetário descentralizado, o Ethereum se caracteriza por seu papel como plataforma programável dentro do ecossistema *blockchain* (LUCENA; HENRIQUES, 2016; BUTERIN, 2014).

5.7 Síntese dos resultados comparativos

A análise comparativa entre Bitcoin e Ethereum evidencia que, embora ambas as redes compartilhem fundamentos comuns da tecnologia *blockchain*, suas arquiteturas foram desenvolvidas para atender a propósitos distintos. O Bitcoin foi concebido com foco na transferência descentralizada de valor, priorizando segurança,

previsibilidade e resistência à censura. O Ethereum, por sua vez, ampliou essa proposta ao incorporar uma infraestrutura programável voltada à execução de contratos inteligentes e aplicações descentralizadas (NAKAMOTO, 2008; BUTERIN, 2014).

As diferenças observadas ao longo deste capítulo confirmam que essas escolhas iniciais de projeto influenciam diretamente o funcionamento de cada rede. O modelo de UTXOs do Bitcoin se ajusta à lógica de um sistema monetário descentralizado, enquanto o modelo de contas do Ethereum favorece a manutenção de estado persistente e a execução de regras programáveis. Da mesma forma, a permanência do Bitcoin na prova de trabalho reforça uma concepção de segurança baseada em custo computacional e energético, enquanto o Ethereum, ao adotar a prova de participação, passou a sustentar sua segurança por meio de validadores e do bloqueio de capital dentro do próprio protocolo (NAKAMOTO, 2008; WOOD, 2025).

Para sintetizar os principais resultados discutidos ao longo deste capítulo, o Quadro 1 apresenta uma comparação entre Bitcoin e Ethereum com base nos critérios técnicos analisados.

Quadro 1 – Síntese comparativa entre Bitcoin e Ethereum

Critério	Bitcoin	Ethereum
Propósito principal	Transferência descentralizada de valor.	Infraestrutura programável para contratos inteligentes e aplicações descentralizadas.
Filosofia de design	Foco em segurança, previsibilidade e especialização monetária.	Foco em programabilidade e diversidade de aplicações.
Modelo transacional	Baseado em UTXOs.	Baseado em contas.
Gestão de estado	Estado associado ao conjunto de saídas não gastas.	Estado global composto por contas e contratos.
Execução programável	*Script* limitado.	EVM com execução de contratos inteligentes.
Mecanismo de consenso	*Proof-of-Work* (PoW).	*Proof-of-Stake* (PoS).
Base da segurança	Trabalho computacional e custo energético.	Validação por *stake* e risco de perda do capital bloqueado.
Escalabilidade	Soluções de segunda camada, com destaque para a *Lightning Network.*	Soluções de segunda camada, com destaque para *rollups*.

Privacidade e auditabilidade	Pseudonimato com rastreabilidade pública das transações.	Transparência pública com rastreabilidade de transações e execuções de contratos.
Principais aplicações	Transferência e preservação descentralizada de valor.	Contratos inteligentes, tokens, finanças descentralizadas e aplicações descentralizadas.

Fonte: Elaborado pelo autor.

6 CONCLUSÃO

Este trabalho teve como objetivo analisar comparativamente Bitcoin e Ethereum, buscando compreender como duas das principais redes do ecossistema *blockchain*, embora baseadas em fundamentos tecnológicos semelhantes, foram desenvolvidas para atender a propósitos distintos. Para isso, inicialmente foram apresentados os conceitos fundamentais da tecnologia *blockchain*, como estrutura de blocos, funções *hash*, rede *peer-to-peer*, mecanismos de consenso, mineração, chaves criptográficas, transações, privacidade e contratos inteligentes. Em seguida, foram examinadas separadamente as arquiteturas do Bitcoin e do Ethereum, de modo a construir a base necessária para a análise comparativa realizada no capítulo final.

A partir dessa análise, verificou-se que o Bitcoin foi criado principalmente como um sistema descentralizado de transferência de valor, com forte ênfase em segurança, previsibilidade e resistência à censura. Sua arquitetura, baseada no modelo de UTXOs, na prova de trabalho e em uma linguagem de *script* limitada, favorece a robustez do sistema monetário descentralizado, ainda que imponha restrições à programabilidade e à ampliação de casos de uso diretamente na camada principal. Dessa forma, o Bitcoin se consolida como uma rede fortemente associada à transferência e à preservação descentralizada de valor.

No caso do Ethereum, observou-se que sua proposta amplia as possibilidades da *blockchain* ao incorporar uma infraestrutura programável capaz de executar contratos inteligentes e sustentar aplicações descentralizadas. Sua arquitetura, baseada em modelo de contas, estado global, *Ethereum Virtual Machine*, mecanismo de *gas* e consenso em *Proof-of-Stake*, evidencia uma rede mais flexível e abrangente. Com isso, o Ethereum se destaca como base para contratos inteligentes, *tokens* e diferentes aplicações desenvolvidas sobre *blockchain*.

A comparação entre as duas redes demonstrou que suas diferenças não devem ser interpretadas em termos absolutos de superioridade, mas sim como resultado de escolhas de projeto voltadas a finalidades distintas. O Bitcoin privilegia simplicidade arquitetural, segurança monetária e resistência à censura, enquanto o Ethereum prioriza programabilidade, manutenção de estado persistente e diversidade de aplicações. Essas diferenças se manifestam no modelo transacional, no mecanismo de consenso, nas estratégias de escalabilidade, nas limitações e possibilidades de privacidade e no espectro de aplicações de cada rede.

Também foi possível observar que tanto Bitcoin quanto Ethereum enfrentam desafios relacionados à escalabilidade e à privacidade. Em ambos os casos, as limitações da camada principal levaram ao desenvolvimento de soluções complementares, como a *Lightning Network* no Bitcoin e os *rollups* no Ethereum. Isso mostra que a evolução prática da tecnologia *blockchain* depende não apenas da camada base, mas também da articulação com mecanismos adicionais capazes de ampliar a capacidade de uso das redes sem comprometer segurança e descentralização.

Diante disso, conclui-se que Bitcoin e Ethereum ocupam posições distintas e complementares dentro do ecossistema *blockchain*. O Bitcoin permanece como referência de sistema monetário descentralizado, enquanto o Ethereum se consolida como infraestrutura programável para contratos inteligentes e aplicações descentralizadas. Assim, a principal conclusão deste trabalho é que a comparação entre essas redes deve ser orientada não por uma lógica de substituição entre elas, mas pela compreensão de que ambas respondem a necessidades diferentes e representam caminhos distintos de evolução da tecnologia *blockchain*.

Como possibilidade de continuidade da pesquisa, sugere-se o aprofundamento da comparação entre Bitcoin e Ethereum com base em indicadores empíricos, como consumo energético, custo médio de transações, desempenho de soluções de segunda camada, níveis de descentralização e padrões de adoção em diferentes contextos. Também pode ser relevante ampliar o estudo para incluir outras redes *blockchain*, permitindo situar Bitcoin e Ethereum em um panorama comparativo mais amplo dentro da evolução dessa tecnologia.

REFERÊNCIAS

AKIAU, Amanda Mendes. **Desenvolvimento de um smart contract para crowdfunding utilizando a rede de blockchain ethereum**. 2023. Trabalho de Conclusão de Curso (Graduação em Engenharia de Controle e Automação) – Universidade Federal de Santa Catarina, Campus Blumenau, Blumenau, 2023. Disponível em: https://repositorio.ufsc.br/handle/123456789/248763. Acesso em: 20 mar. 2026.

ALVES, Abadimarques Queiroz Aquino. **Regulamentação das criptomoedas: aspectos jurídicos da moeda do amanhã**. 2022. Trabalho de Conclusão de Curso – Pontifícia Universidade Católica de Goiás, Goiânia, 2022. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3960. Acesso em: 01 set. 2025.

ANTONOPOULOS, Andreas M.; HARDING, David A. **Mastering Bitcoin: programming the open blockchain**. 3. ed. Sebastopol, CA: O'Reilly Media, 2023. Disponível em: https://github.com/bitcoinbook/bitcoinbook. Acesso em: 28 fev. 2026.

ANTONOPOULOS, Andreas M.; WOOD, Gavin. **Mastering Ethereum: building smart contracts and DApps**. Sebastopol, CA: O'Reilly Media, 2018.

BUTERIN, Vitalik. **Ethereum: a next-generation smart contract and decentralized application platform**. [S. l.: s. n.], 2014. Disponível em: https://ethereum.org/content/whitepaper/whitepaper-pdf/Ethereum_Whitepaper_-_Buterin_2014.pdf. Acesso em: 13 mar. 2026.

CARDOSO, Alana Almeida; PEDROSA, Douglas Fuck; MACEDO, Lucas Rodrigues de; RINALDI, Nicole Christine; FREITAS, Renato Panchihak Bueno de; GOEDERT, Yohann Godoy; SANTOS, Christiane Bischof dos. **Da tecnologia blockchain e smart contracts nas organizações: um estudo multicasos em Curitiba**. Memorial TCC Caderno da Graduação, Curitiba, v. 6, n. 1, p. 9-26, 2020. Disponível em: https://memorialtcccadernograduacao.fae.edu/cadernotcc/article/view/291. Acesso em: 18 nov. 2025.

CHERVINSKI, João Otávio Massari; KREUTZ, Diego. **Introdução às tecnologias dos blockchains e das criptomoedas**. Revista Brasileira de Computação Aplicada, Passo Fundo, v. 11, n. 3, p. 12-27, 2019. DOI: https://doi.org/10.5335/rbca.v11i3.9394. Disponível em: https://ojs.upf.br/index.php/rbca/article/view/9394. Acesso em: 01 out. 2025.

ETHEREUM.ORG. **Cancun-Deneb (Dencun) FAQ**. [S. l.: s. n.], 2025a. Disponível em: https://ethereum.org/roadmap/dencun/. Acesso em: 21 mar. 2026.

ETHEREUM.ORG. **Optimistic Rollups**. [S. l.: s. n.], 2026a. Disponível em: https://ethereum.org/developers/docs/scaling/optimistic-rollups/. Acesso em: 21 mar. 2026.

ETHEREUM.ORG. **Scaling**. [S. l.: s. n.], 2026b. Disponível em: https://ethereum.org/developers/docs/scaling/. Acesso em: 21 mar. 2026.

ETHEREUM.ORG. **What is layer 2?** [S. l.: s. n.], 2025b. Disponível em: https://ethereum.org/layer-2/learn/. Acesso em: 21 mar. 2026.

ETHEREUM.ORG. **Zero-knowledge rollups**. [S. l.: s. n.], 2026c. Disponível em: https://ethereum.org/developers/docs/scaling/zk-rollups/. Acesso em: 21 mar. 2026.

FERREIRA, Juliandson Estanislau; PINTO, Filipe Gutemberg Costa; SANTOS, Simone Cristiane dos. **Estudo de mapeamento sistemático sobre as tendências e desafios do blockchain**. GESTÃO.Org, Recife, v. 15, ed. especial, p. 108-117, 2017. DOI: 10.21714/1679-18272017v15Ed.p108-117. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7328726. Acesso em: 22 set. 2025.

FIGUEIREDO, Jordan E. M.; LIMA, Iremar N. **Contratos inteligentes com Ethereum**. Journal of Innovation and Science: research and application, [S. l.], v. 1, n. 1, p. 38-48, 2021. DOI: https://doi.org/10.56509/joins.2021.v1.98. Disponível em: https://joins.emnuvens.com.br/joins/article/view/98. Acesso em: 06 out. 2025.

GRANDJEAN, Dominic; HEIMBACH, Lioba; WATTENHOFER, Roger. Ethereum proof-of-stake consensus layer: participation and decentralization. [S. l.: s. n.], 2023. arXiv:2306.10777. DOI: 10.48550/arXiv.2306.10777. Disponível em: https://arxiv.org/abs/2306.10777. Acesso em: 26 mar. 2026.

GÜNDLACH, Rowel; STOEPKER, Ivo V.; KAPODISTRIA, Stella; RESING, Jacques A. C. **A holistic approach for Bitcoin confirmation times & optimal fee selection**. [S. l.: s. n.], 2024. arXiv:2402.17474. DOI: 10.48550/arXiv.2402.17474. Disponível em: https://arxiv.org/abs/2402.17474. Acesso em: 05 mar. 2026.

KUO, Tsung-Ting; KIM, Hyeon-Eui; OHNO-MACHADO, Lucila. **Blockchain distributed ledger technologies for biomedical and health care applications**. Journal of the American Medical Informatics Association, [S. l.], v. 24, n. 6, p. 1211-1220, nov. 2017. DOI: 10.1093/jamia/ocx068. Disponível em: https://academic.oup.com/jamia/article/24/6/1211/4108087. Acesso em: 14 mar. 2026.

LUCENA, Antônio Unias de; HENRIQUES, Marco Aurélio Amaral. **Estudo de arquiteturas dos blockchains de Bitcoin e Ethereum.** In: ENCONTRO DE ALUNOS E DOCENTES DO DCA/FEEC/UNICAMP (EADCA), 9., 2016, Campinas. Anais [...]. [Campinas, SP]: [FEEC/UNICAMP], 2016. p. 1-4. Disponível em: https://pt.scribd.com/document/377995531/Estudo-de-arquiteturas-dos-blockchains-de-Bitcoin-e-Ethereum. Acesso em: 02 fev. 2026.

MEIKLEJOHN, Sarah; POMAROLE, Marjori; JORDAN, Grant; LEVCHENKO, Kirill; MCCOY, Damon; VOELKER, Geoffrey M.; SAVAGE, Stefan. **A fistful of bitcoins: characterizing payments among men with no names**. In: INTERNET MEASUREMENT CONFERENCE (IMC '13), 2013, Barcelona. Proceedings of the 2013 conference on Internet measurement conference. New York, NY: Association for Computing Machinery, 2013. p. 127-140. DOI:

https://doi.org/10.1145/2504730.2504747. Disponível em: https://dl.acm.org/doi/10.1145/2504730.2504747. Acesso em: 10 mar. 2026.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. [S. l.: s. n.], 2008. 9 p. Disponível em: https://bitcoin.org/bitcoin.pdf. Acesso em: 16 nov. 2025.

NORMAN, Alan T. **Dominar a bitcoin para principiantes: a bitcoin, as tecnologias de criptomoedas, a mineração, o investimento e a negociação**. [S. l.]: Tektime, 2020.

OLIVÉ, Antoni. **The conceptual schema of Ethereum and of the ERC–20 token standard**. [S. l.: s. n.], 2020. Disponível em: https://upcommons.upc.edu/bitstreams/31abfb39-927b-474d-83f4-951fabaa843f/download. Acesso em: 21 mar. 2026.

PIMENTEL, Daniel de Melo. **Uma proposta para aprimorar o anonimato em transações bitcoin com suporte à auditoria**. 2017. 94 f. Dissertação (Mestrado em Informática) – Instituto de Computação. Programa de Pós-Graduação em Informática, Universidade Federal de Alagoas, Maceió, 2017. Disponível em: https://www.repositorio.ufal.br/handle/riufal/1963. Acesso em: 12 dez. 2025.

POON, Joseph; DRYJA, Thaddeus. **The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments**. 2016. Whitepaper. Disponível em: https://nakamotoinstitute.org/library/lightning-network/. Acesso em: 10 mar. 2026.

SENDIN, Ivan da Silva; MIANI, Rodrigo Sanches; RIBEIRO, Pedro Henrique Resende. **Análise Forense aplicada ao Bitcoin**. In: MARCONDES, Cesar Augusto Cavalheiro; MANSILHA, Rodrigo Brandão; KREUTZ, Diego; PEREIRA JUNIOR, Lourenço Alves (org.). Minicursos do XXIV Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais. Porto Alegre: Sociedade Brasileira de Computação, 2024. p. 132-179. DOI: https://doi.org/10.5753/sbc.15101.8. Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/book/151. Acesso em: 02 mar. 2026.

SEMLER SCIENTIFIC, INC. **Bitcoin strategy related supplemental disclosures**. [S. l.: s. n.], 2024. Disponível em: https://www.sec.gov/Archives/edgar/data/1554859/000110465924079094/tm2416433d5_ex99-1.htm. Acesso em: 28 mar. 2026.

WOOD, Gavin. **ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER**. Shanghai version efc5f9a – 2025-02-04. [S. l.: s. n.], 2025. Disponível em: https://ethereum.github.io/yellowpaper/paper.pdf. Acesso em: 15 mar. 2026.

Pontifícia Universidade Católica de Goiás
Pontifical Catholic University of Goias
Av. Universitária, 1069, Setor Universitário
Caixa Postal 86 - CEP 74.605-010
Goiânia – Goiás – Brasil

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Sergio Jose de Almeida Filho do Curso de Ciência da Computação matrícula 20212002800484 telefone: 62996985062, e-mail sergiofilho0609@hotmail.com , na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado CRIPTOMOEDAS E BLOCKCHAIN: UMA ANÁLISE COMPARATIVA ENTRE BITCOIN E ETHEREUM, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 23 de Junho de 2026.

Documento assinado digitalmente
gov.br SERGIO JOSE DE ALMEIDA FILHO
Data: 23/06/2026 14:15:08-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: Sergio José de Almeida Filho

Documento assinado digitalmente
gov.br EUGENIO JULIO MESSALA CANDIDO CARVALHO
Data: 24/06/2026 10:57:12-0300
Verifique em https://validar.iti.gov.br

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: Eugênio Júlio Messala Cândido Carvalho