Universidade Federal dos Vales do Jequitinhonha e Mucuri

Faculdade de Ciências Exatas e Tecnológicas

Departamento de Computação

Curso de Sistemas de Informação

Estudo sobre a tecnologia Blockchain, uma análise comparativa entre o Bitcoin e Ethereum

Vinícius Soares de Paula Souza

Diamantina

2023

Universidade Federal dos Vales do Jequitinhonha e Mucuri

Faculdade de Ciências Exatas e Tecnológicas

Departamento de Computação

Curso de Sistemas de Informação

Estudo sobre a tecnologia Blockchain, uma análise comparativa entre o Bitcoin e Ethereum

Vinícius Soares de Paula Souza

Monografia apresentada ao Curso de Sistemas de Informação do Departamento de Computação da Universidade Federal dos Vales do Jequitinhonha e Mucuri como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Marcelo Ferreira Rego

Diamantina

2023

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DOS VALES DO JEQUITINHONHA E MUCURI

FOLHA DE APROVAÇÃO

Vinícius Soares de Paula Souza

ESTUDO SOBRE A TECNOLOGIA BLOCKCHAIN, UMA ANÁLISE COMPARATIVA ENTRE O BITCOIN E ETHEREUM

Trabalho de Conclusão de Curso apresentado ao Departamento de Computação como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação pela Universidade Federal dos Vales do Jequitinhonha e Mucuri.

Aprovada em 31/01/2023

BANCA EXAMINADORA

Prof. Marcelo Ferreira Rego
Faculdade de Ciências Exatas - UFVJM

Profa. Cinthya Rocha Tameirão
Faculdade de Ciências Exatas - UFVJM

Prof. Erinaldo Barbosa da Silva
Faculdade de Ciências Exatas - UFVJM

Documento assinado eletronicamente por **Cinthya Rocha Tameirão**, **Servidor (a)**, em 31/01/2023, às 16:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Marcelo Ferreira Rego**, **Servidor (a)**, em 07/02/2023, às 13:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Erinaldo Barbosa da Silva**, **Servidor (a)**, em 08/02/2023, às 11:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ufvjm.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0961337** e o código CRC **BF8CEE03**.

Dedico este trabalho a minha família, amigos e a todos que estiveram comigo, me apoiaram e incentivaram durante essa jornada.

Agradecimentos

Em primeiro lugar, agradeço aos meus pais que sempre me apoiaram e me incentivaram, além de sempre acreditarem em mim desde muito cedo e na importância que a educação teria em minha vida. Agradeço também a minha família e amigos, que estiveram comigo durante toda essa jornada e me deram forças pra continuar. E por fim, agradeço a todos os meus professores e colegas de curso, juntos compartilhamos conhecimentos e experiências que levarei para toda a vida.

"Onde a ignorância se esconde, também estão as fronteiras da descoberta e da imaginação."(Neil deGrasse Tyson)

Resumo

A Blockchain surgiu a partir da união de diversos conceitos e tecnologias, com o objetivo de criar a primeira moeda digital descentralizada, o Bitcoin. Esse novo tipo de ativo é denominado como criptomoeda. Com o passar do tempo surgiram outras criptomoedas, entre elas, o Ethereum, que se destaca pelo uso combinado da tecnologia Blockchain com contratos inteligentes, favorecendo a consolidação e sua aplicação em diversas áreas. Atualmente, as criptomoedas são uma alternativa as formas tradicionais de pagamento, por exemplo, as moedas fiduciárias. Como vantagem elas permitem uma maior privacidade, descentralização das transações, são mais acessíveis, eficientes, além de possibilitar a criação de aplicações financeiras descentralizadas. Considerando a importância dessa nova tecnologia no contexto atual, o presente trabalho tem como objetivo apresentar um estudo a respeito da Blockchain, criptomoedas e seus diversos aspectos como, conceito, história, funcionamento e economia. Além de realizar um estudo comparativo entre as duas principais criptomoedas do mercado: o Bitcoin e o Ethereum. Após a realização desse estudo, os resultados indicam que o Bitcoin e Ethereum compartilham de elementos em comum. Porém, se diferem em alguns aspectos, como: histórico, escopo, desenvolvimento, funcionamento e aspectos econômicos.

Palavras-chaves: Blockchain. Criptomoeda. Bitcoin. Ethereum. Contratos inteligentes.

Abstract

The Blockchain emerged from the union of several concepts and technologies, intending to create the first decentralized digital currency, Bitcoin. This new type of asset is called cryptocurrency. Over time, other cryptocurrencies emerged, including Ethereum, which stands out for its combined use of Blockchain technology with smart contracts, favoring consolidation and its application in several areas. Currently, cryptocurrencies are an alternative to traditional forms of payment, for example, fiat currencies. As an advantage, they allow greater privacy and decentralization of transactions, making them more accessible and efficient, in addition to enabling the creation of decentralized financial applications. Considering the importance of this new technology in the current context, the present work aims to present a study on Blockchain, cryptocurrencies, and its various aspects such as concept, history, functioning, and economy. In addition to doing a comparative study between the two main cryptocurrencies in the market: Bitcoin and Ethereum. After carrying out this study, the results indicate that Bitcoin and Ethereum share common elements. However, they differ in some aspects, such: as history, scope, development, functioning, and economics.

Key-words: Blockchain. Cryptocurrency. Bitcoin. Ethereum. Smart contracts.

Lista de Ilustrações

Figura 1 – Envio de mensagem - Criptografia simétrica (SAKURAI, 2020) 6
Figura 2 – Envio de mensagem - Criptografia assimétrica (PINTO, 2010) 7
Figura 3 – Funcionamento da assinatura digital (ACDX, 2008) 9

Figura 4 – Nó completo e suas funções (ANTONOPOULOS, 2019) 18
Figura 5 – Tipos de nós na rede Bitcoin. Adaptada de Antonopoulos (2019) 19
Figura 6 – Rede do Bitcoin estendida (ANTONOPOULOS, 2019) 20
Figura 7 – Endereço Bitcoin (WANDER, 2013a) 21
Figura 8 – Transações no Bitcoin: entradas e saídas (WANDER, 2013c) 23
Figura 9 – Cadeia de transações. Adaptada de (NAKAMOTO, 2008) 24
Figura 10 – Organização da cadeia de blocos (Blockchain). (LIMA, 2020) 25
Figura 11 – Estrutura de uma Merkle Tree(ANTONOPOULOS, 2019) 26
Figura 12 – Cadeia de blocos(WANDER, 2013b) 27
Figura 13 – *Hark Fork* (ANTONOPOULOS, 2019) 31
Figura 14 – Ethereum: *The Merge* (NAIJA, 2022) 46
Figura 15 – *Web3*: Uma web descentralizada usando contratos inteligentes e tecnologias P2P (ANTONOPOULOS; WOOD, 2018) 49

Figura 16 – Internet vs Crypto Adoption (WAN, 2021) 54
Figura 17 – Valor do Bitcoin (COINMARKETCAP, 2022) 54
Figura 18 – Capitalização do mercado de criptomoedas (COINDANCE, 2022) 55
Figura 19 – Capitalização por criptomoedas (COINDANCE, 2022) 55
Figura 20 – Índice do Dólar de 2013 a 2022 (TRADINGECONOMICS, 2022) 56
Figura 21 – Valor do Ouro de 2013 a 2022 (TRADINGECONOMICS, 2022) 57

Figura 22 – Preço do Bitcoin e Ethereum de 2019 à 2023 (COINMARKETCAP, 2023) . 63
Figura 23 – Taxas de transação (THEBLOCK, 2023) 64
Figura 24 – Número de transações (THEBLOCK, 2023) 64
Figura 25 – Número de endereços ativos (THEBLOCK, 2023) 65

Lista de Tabelas

Tabela 1 – Estrutura do bloco 26
Tabela 2 – Estrutura do cabeçalho de um bloco 27

Lista de Abreviaturas e Siglas

P2P	*Peer-to-peer*
TI	*Tecnologia da Informação*
BTC	*Bitcoin*
CTO	*Chief Technology Officer*
CPU	*Central Processing Unit*
SPV	*Simplified Payment Verification*
SHA256	*Algoritmo de hash*
RIPEMD160	*Algoritmo de hash*
IBAN	*International Bank Account Number*
PoW	*Proof-of-work*
UTM	*Universal Turing Machine*
EVM	*Ethereum Virtual Machine*
ETH	*Ether*
EOA	*Externally Owned Account*
DApp	*Decentralized Application*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
ID	*Identity*
PoS	*Proof-of-stake*
Fiat	*Fiduciárias*
DEX	*Decentralized Exchange*
B2B	*Business-to-business*
USD	*United States Dollar*
Market Cap	*Market Capitalization*

Sumário

1 Introdução 1

2 Metodologia 3
2.1 Tipo de pesquisa 3
2.2 Processo de pesquisa 3
2.2.1 Planejamento 3
2.2.2 Condução 3
2.2.3 Documentação 4

3 Referencial teórico 5
3.1 Criptografia 5
3.1.1 Função Hash 7
3.1.2 Assinatura digital 8
3.2 Redes P2P 10
3.3 Criptomoedas 10
3.3.1 Definição 10
3.3.2 Surgimento 11
3.3.2.1 Bitcoin 13
3.3.2.2 Ethereum 14
3.3.3 Carteiras 15
3.3.4 Mineração 16

4 Funcionamento das criptomoedas 17
4.1 Bitcoin 17
4.1.1 Blockchain 17
4.1.2 Nós da rede 18
4.1.3 Endereços 21
4.1.4 Carteiras 22
4.1.5 Transações 22
4.1.6 Blocos 25
4.1.7 Mineração 28
4.1.8 *Forks* 30
4.1.9 Altcoins 31
4.1.10 Visão geral 33

4.2 Ethereum . . . 35
4.2.1 Blockchain . . . 35
4.2.2 Turing completude e Ethereum . . . 36
4.2.3 Unidades de moeda . . . 37
4.2.4 Contas de propriedade externa e contratos . . . 37
4.2.5 Clientes . . . 38
4.2.6 Carteiras . . . 39
4.2.7 Transações e mensagens . . . 40
4.2.8 Blocos . . . 43
4.2.9 Contratos inteligentes e Solidity . . . 43
4.2.10 Tokens . . . 44
4.2.11 Mineração . . . 45
4.2.12 *Proof of Stake* . . . 47
4.2.13 DApps . . . 48
4.2.14 Moedas alternativas ao Ethereum . . . 50
4.2.15 Visão geral . . . 50

5 Aspectos econômicos . . . 53
5.1 Criptomoedas e moedas Fiat . . . 53
5.2 Utilização das criptomoedas . . . 53
5.3 Investimentos em criptomoedas . . . 54
5.3.1 Mercado e valor . . . 56
5.4 Ecossistema financeiro . . . 57
5.4.1 Corretoras descentralizadas . . . 58
5.4.2 Carteiras . . . 58
5.4.3 Serviços de pagamento . . . 59
5.4.4 Mineração . . . 59

6 Análise comparativa: Bitcoin e Ethereum . . . 61
6.1 Histórico . . . 61
6.2 Escopo e desenvolvimento . . . 61
6.3 Funcionamento . . . 62
6.4 Aspectos financeiros . . . 63

7 Conclusão . . . 67
7.1 Trabalhos futuros . . . 68

Referências . . . 69

1 Introdução

A tecnologia Blockchain ou cadeia de blocos é um sistema descentralizado de registro de dados, que utiliza tecnologias como as redes P2P e a criptografia para armazenar e processar transações de forma segura, eliminando assim, a necessidade de uma entidade centralizadora para gerenciar as transações. A tecnologia Blockchain pode ser usada em diversas aplicações, atualmente, o seu principal uso são as criptomoedas.

As criptomoedas são moedas digitais que possuem como base uma Blockchain e são uma alternativa as moedas fiduciárias. Atualmente, são amplamente utilizadas como meio de pagamento e reserva de valor. No momento presente, a capitalização global do mercado de criptomoedas ultrapassa 840 bilhões de dólares. (COINMARKETCAP, 2023).

O Bitcoin e Ethereum são as criptomoedas com a maior capitalização do mercado, sendo que o Bitcoin ultrapassa os 360 bilhões de dólares e o Ethereum, 170 bilhões de dólares. (COINMARKETCAP, 2023). Considerando a relevância do tema, o objetivo desse trabalho é realizar um estudo a cerca da tecnologia Blockchain, além de uma análise comparativa entre essas duas criptomoedas.

Diante disso, este trabalho tem como objetivo geral apresentar um estudo a cerca da tecnologia Blockchain e uma análise comparativa entre as criptomoedas Bitcoin e Ethereum, considerando os aspectos técnicos e econômicos de cada uma.

Para alcançar esse objetivo, forma traçados objetivos específicos: apresentar o conceito de criptomoedas, caracterizar o Bitcoin e Ethereum, especificar o conceito e funcionamento da Blockchain bem como o funcionamento do Bitcoin e Ethereum, apontar alguns dos aspectos econômicos das criptomoedas e comparar o Bitcoin e Ethereum de acordo com os aspectos apresentados neste trabalho.

O trabalho está dividido em seis capítulos. O Capítulo 1 (o presente capítulo), apresenta uma introdução para o trabalho. O Capítulo 2 apresenta os conceitos iniciais a respeito das criptomoedas. O Capítulo 3 apresenta um referencial teórico a respeito do tema. O Capítulo 4 trata do funcionamento do Bitcoin e Ethereum. O Capítulo 5 trata dos aspectos econômicos das criptomoedas, o Capítulo 6 apresentas a análise comparativa entre o Bitcoin e o Ethereum, e , por fim, as considerações finais são apresentadas no Capítulo 7.

2 Metodologia

Este estudo se baseou em uma abordagem qualitativa de pesquisa, de natureza básica, com o objetivo exploratório, por meio de uma pesquisa bibliográfica. Este capítulo tem como objetivo, abordar os procedimentos metodológicos do tipo de pesquisa utilizado.

2.1 Tipo de pesquisa

Devido ao objetivo deste trabalho que é realizar um estudo a cerca da tecnologia Blockchain e uma análise comparativa entre o Bitcoin e Ethereum, a abordagem de pesquisa adotada foi a qualitativa de caráter exploratório. De acordo com Vergara (1990), a pesquisa exploratória trata-se de uma investigação em uma área que há pouco conhecimento sistematizado ou acumulado. Além disso, pela sua natureza de sondagem o caráter exploratório não comporta hipóteses prévias que poderão surgir durante ou ao final da pesquisa.

Com relação aos procedimentos de pesquisa, o procedimento adotado foi a pesquisa bibliográfica. Segundo Vergara (1990) trata-se de um estudo sistematizado desenvolvido a partir de material publicado em livros, revistas, jornais, ou seja, material acessível ao público geral.

2.2 Processo de pesquisa

Para o desenvolvimento desse trabalho foram adotadas as seguintes etapas:

2.2.1 Planejamento

A etapa de planejamento é onde de acordo com o tema do trabalho, foram definidos os tópicos a serem pesquisados e posteriormente, abordados no texto. Neste caso, o tema do trabalho é "Estudo sobre a tecnologia Blockchain, uma análise comparativa entre o Bitcoin e Ethereum".

2.2.2 Condução

A etapa de condução é onde foi realizada a pesquisa e a seleção dos materiais (livros, páginas, artigos, etc). A pesquisa se deu principalmente em periódicos e mecanismos de busca de artigos e livros. A seleção foi feita tendo como base a abordagem dada pelos materiais aos tópicos definidos na etapa de planejamento. Uma observação importante é que muitos dos materiais mais completos encontrados não estavam na língua portuguesa mas em inglês.

2.2.3 Documentação

A etapa de documentação é onde o estudo foi elaborado, buscando realizar um compilado a respeito dos tópicos definidos na etapa de planejamento, usando como base os materiais selecionados na etapa de condução.

3 Referencial teórico

Este capítulo visa especificar o conceito de carteiras e mineração, uma vez que são conceitos fundamentais para uma melhor compreensão à respeito das criptomoedas. Além disso, esse capítulo visa apresentar o conceito de criptografia e redes ponto a ponto, já que estes são componentes da Blockchain e permitem que ela seja uma rede segura, descentralizada e confiável para armazenamento e transferência de dados.

3.1 Criptografia

Cryptos é uma palavra de origem grega que significa secreto ou oculto. A criptografia estuda, dentre outras coisas, os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos". (COUTINHO, 2016, p. 1).

Conforme Okumura et al. (2014) explica, o primeiro uso documentado da criptografia teria sido feito em 1900 a.c., no Egito. Ela foi criada com o objetivo de esconder mensagens, bem como o seus significados, para que somente os seus destinatários pudessem decifrá-las.

Assim, a criptografia pode ser usada para tornar sigilosa a comunicação entre duas ou mais pessoas. Para garantir esse sigilo, os algoritmos de criptografia camuflam as mensagens, tornando as mesmas não legíveis para possíveis espiões que consiga interceptá-las. Segundo Okumura et al. (2014), existem diversas formas de se camuflar uma mensagem, uma delas é feita usando uma chave que embaralha o conteúdo da mensagem e gera uma saída diferente da original.

Desse modo, segundo Oliveira (2012) a segurança da informação possui seis fundamentos, que os algoritmos de criptografia, assim como as demais técnicas de segurança da informação visam atender. São eles:

- Disponibilidade - visa garantir que uma informação esteja disponível para o acesso quando for necessária.
- Integridade - visa garantir que o conteúdo da mensagem permaneça íntegro.
- Controle de acesso - visa garantir que a informação só seja acessada por quem tem autorização para tal.
- Autenticidade - visa garantir a identidade do emissor da mensagem.
- Não-repudiação - visa prevenir que alguém negue o envio ou recebimento de uma mensagem.

- Privacidade - visa garantir que somente o emissor e receptor tenham conhecimento da mensagem.

Os algoritmos criptográficos podem ser classificados de diversas formas. (SANTOS, 2018). Uma dessas classificações, é baseada na quantidade de chaves usadas, tendo assim a criptografia simétrica e assimétrica. Na criptografia simétrica utiliza-se apenas uma chave, logo ambos, emissor e receptor, devem conhecê-la, um para encriptar e outro para decriptar a mensagem. As vantagens desse método, segundo Oliveira (2012) é a simplicidade, já que o mesmo possui um uso facilitado e rapidez para execução dos processos criptográficos. Porém, na criptografia simétrica ambos, o emissor e o receptor, devem compartilhar a mesma chave criptográfica, isso pode ser um problema, pois cria a necessidade de um meio seguro para tal. Além da necessidade de ambos manterem a chave em sigilo.

A Figura 1 mostra um esquema do envio de uma mensagem, baseado na criptografia de chave simétrica:

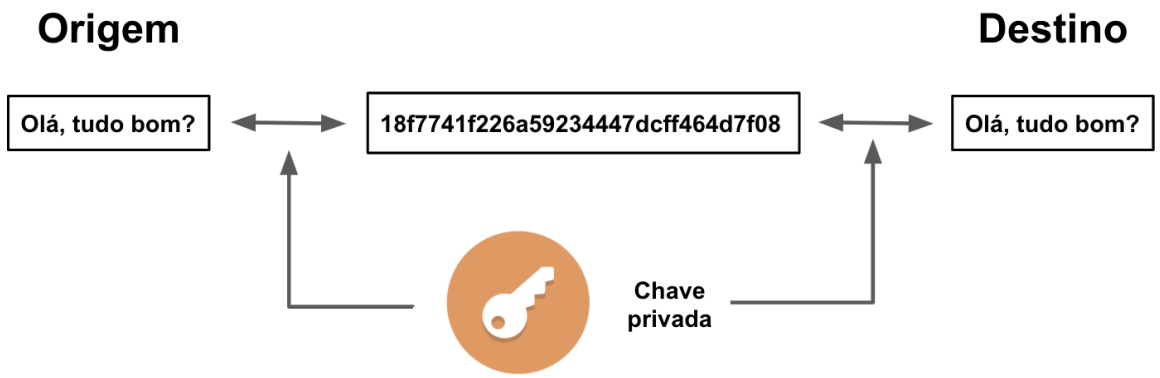

Figura 1 – Envio de mensagem - Criptografia simétrica (SAKURAI, 2020)

No esquema apresentado na Figura 1, a mensagem ”Olá, tudo bom?” é criptografada na origem usando uma chave privada, enviada e por fim descriptografada no destino usando a mesma chave.

Já a criptografia assimétrica, conforme apresentado por Santos (2018), utiliza um par de chaves complementares. Na qual ambos, emissor e receptor possuem uma chave pública e privada. E como os nomes sugerem, a chave pública pode ser compartilhada publicamente, e a chave privada deve ser mantida em sigilo. Logo, pode-se usar a chave pública do receptor para encriptar e a privada do mesmo para decriptar.

A Figura 2 mostra um esquema do envio de uma mensagem, baseado na criptografia de chaves assimétricas:

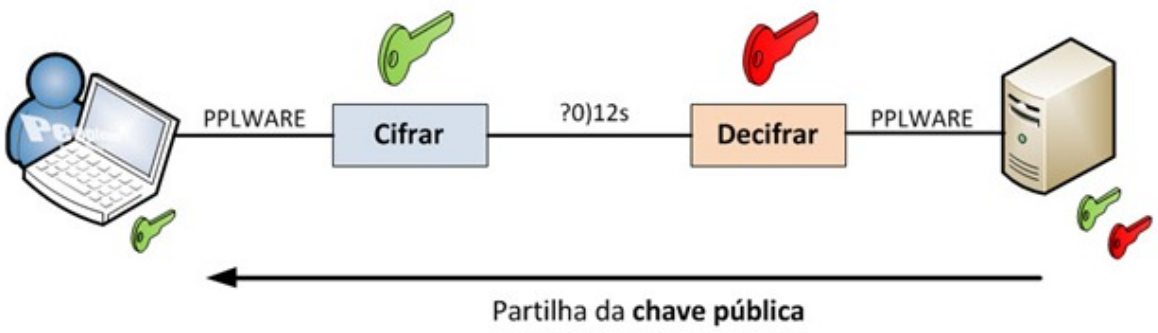

Figura 2 – Envio de mensagem - Criptografia assimétrica (PINTO, 2010)

Na Figura 2 é possível observar que o emissor cifra a mensagem usando a chave pública do receptor (em verde) , que por sua vez, decifra a mensagem usando a sua chave privada (em vermelho).

> Assim, a criptografia assimétrica tende a ser mais confiável, já que ela necessita apenas que o emissor e receptor guardem a sua chave privada em um local seguro para ser efetiva. No entanto, o tempo de processamento de mensagens com criptografia assimétrica é muitas vezes maior do que com criptografia simétrica, o que pode limitar seu uso em determinadas situações (OLIVEIRA, 2012, p. 4).

Souza (2008) explica que as chaves assimétricas são mais lentas no geral por possuírem tarefas matemáticas mais intensas. Porém, o mesmo adverte que seria melhor utilizar a criptografia assimétrica em redes de longa distância e na internet, já que elas garantem os princípios de autenticidade e não-repúdio.

3.1.1 Função Hash

As funções *hash*, como apresentadas por Figueiredo (2020) e Santos (2018) também podem ser chamadas de funções de dispersão criptográfica. As funções *hash* são usadas para gerar saídas de tamanho fixo e criptografadas a partir de entradas de tamanho variável. As saídas dessas funções são chamadas de *hashes* e o seu tamanho é definido pelo algoritmo de *hash*. Além disso, um ponto interessante dessas funções é que qualquer alteração, mesmo que pequena na entrada, gera uma saída completamente diferente.

Sendo assim, como apresentado por Burnett (2002) e Figueiredo (2020), uma função *hash* é considerada efetiva se apresenta as seguintes propriedades:

- É fácil de encontrar a *hash* a partir da entrada, mas é difícil de se encontrar a entrada a partir da *hash*.
- É livre de colisões, ou seja, diferentes entradas não geram uma mesma saída.
- Entradas de tamanhos distintos geram saídas com o mesmo tamanho.

- Pequenas mudanças na entrada geram saídas muito diferentes.

Para Figueiredo (2020) colisão é o nome dado ao evento de se gerar a mesma *hash* a partir de uma mesma entrada. Nesse sentido, são exigidos algoritmos com baixa probabilidade de colisão, já que, na teoria é impossível eliminar esse fenômeno. Uma vez que o as possibilidades de entrada para a função são infinitas, mas as possibilidades de saída, finitas.

3.1.2 Assinatura digital

Conforme Gandini, Salomão e Jacob (2001) apresentam, os documentos digitais possuem características que os diferem de documentos tradicionais. Os mesmos, podem ser fáceis de alterar e falsificar, tornando necessário o uso de técnicas como a assinatura digital, que visa permitir a verificação da integridade e garantir a autenticidade dos dados. Assim, segundo Figueiredo (2020), a assinatura digital é um meio de substituir a assinatura física, tendo como base a criptografia e as funções *hash*. Como Burnett (2002) explica e a Figura 3 apresenta, a assinatura digital funciona da seguinte forma:

1. Primeiro, o emissor utilizando de uma função *hash*, resume a mensagem.
2. Em seguida, usando uma chave privada, o emissor criptografa a mensagem. Esse resumo criptografado é que irá funcionar como assinatura.
3. Assim, o emissor envia a mensagem junto da assinatura.
4. Ao receber a mensagem, o destinatário separa os dois componentes (mensagem e assinatura) e resume a mensagem.
5. Em seguida, ele descriptografa a assinatura usando a chave pública do emissor. Aqui a autenticidade da mensagem pode ser atestada, já que de acordo com as propriedades da criptografia assimétrica, se a assinatura foi descriptografada com a chave pública do emissor, então a única chave que poderia gerar essa assinatura é a chave privada do mesmo.
6. Após descriptografar ele obterá o resumo enviado pelo emissor e poderá comparar com o resumo gerado por ele mesmo, atestando se a integridade da mensagem.

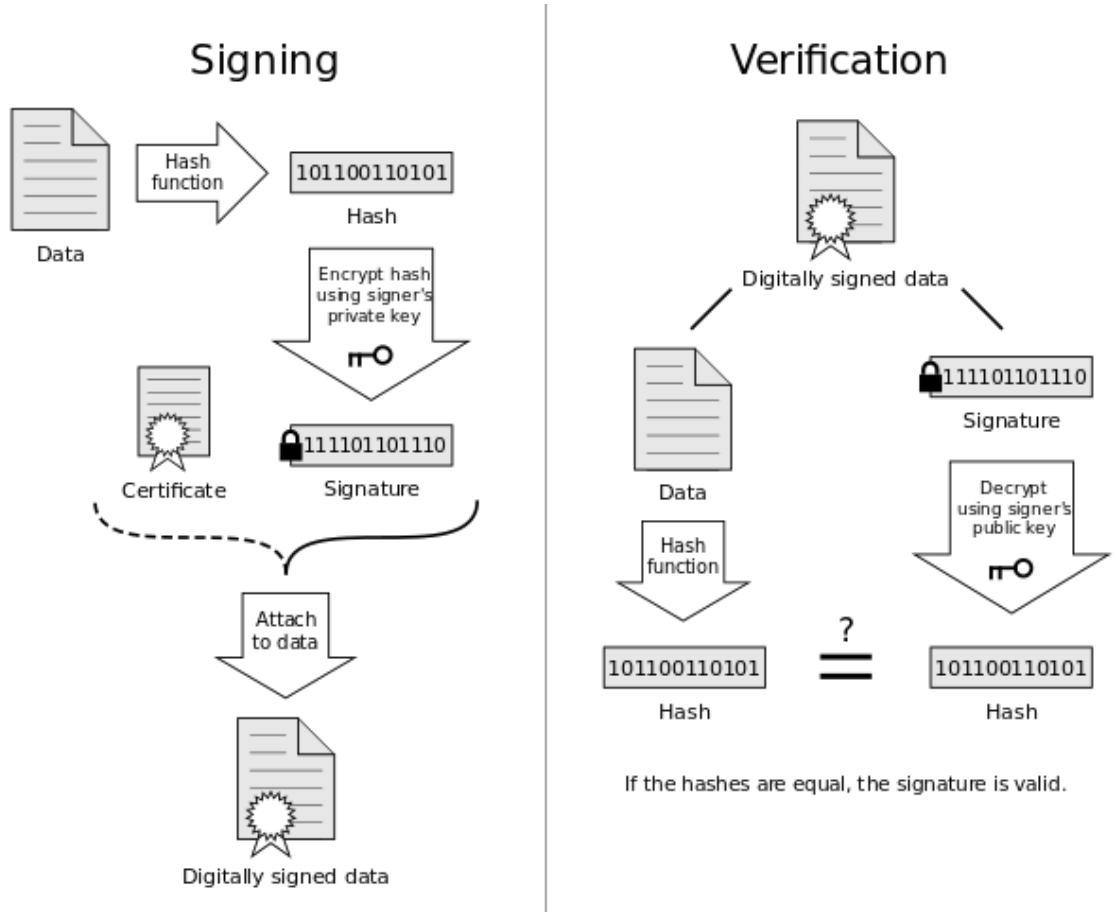

Figura 3 – Funcionamento da assinatura digital (ACDX, 2008)

A Figura 3 apresenta do lado esquerdo as etapas para assinatura de dodos e do lado direito o processo para verificação da assinatura.

Dessa forma, como observado por Burnett (2002) e Figueiredo (2020) é possível checar se os dados foram alterados e se o emissor confirma o conteúdo da mensagem, isso, sem que a chave privada do mesmo seja divulgada. Assim, como Oliveira (2012) explica, os princípios da autenticidade, integridade e não-repudiação são garantidos, uma vez que somente o indivíduo que assinou a mensagem possuía aquela chave privada, correspondente a chave pública usada para decifrar a mensagem.

> Cada assinatura é única para os dados assinados e para as chaves utilizadas. Quando uma pessoa assina duas mensagens diferentes com a mesma chave, as assinaturas serão diferentes. Além disso, quando duas pessoas com chaves diferentes assinam os mesmos dados, elas produzirão assinaturas diferentes. Como resultado disso, alguém não pode pegar uma assinatura válida e acrescentá-la a parte inferior de uma mensagem, algo que torna a falsificação de uma mensagem muito mais difícil (BURNETT, 2002, p. 131).

Além disso, segundo Santos (2018) o uso da função *hash* possibilita ainda, a otimização do uso de assinaturas digitais, já que o processo de criptografia pode demorar muito para cifrar grandes mensagens, mas o resumo é menor e possui um tamanho fixo.

3.2 Redes P2P

Redes *peer-to-peer* estão relacionadas a uma arquitetura de rede que funciona na Internet e possui o objetivo de compartilhar recursos entre os participantes, sendo que por princípio não há diferenciação entre eles. (ROCHA et al., 2004, p. 2). Barcellos e Gaspary (2006) explicam que redes *peer-to-peer*, ou P2P, são constituídas por nós interconectados formando sistemas distribuídos que se organizam para compartilhar conteúdo, como música, vídeos, documentos, etc. Além disso, elas podem compartilhar recursos como ciclos de CPU, armazenamento e largura de banda; mantendo uma conectividade e desempenho, sem ter uma entidade central organizando tudo.

Segundo Sichel e Calixto (2018), há duas formas de se atuar nas redes de computadores. Em uma delas é possível ser o servidor, responsável pelo envio das informações. Em outra, é possível ser o cliente, que recebe as informações transmitidas. Conforme apresentado por Santos (2018) e Brochado (2018), na arquitetura *peer-to-peer*, os participantes funcionam ao mesmo tempo como clientes e servidores. E podem ser também chamados de *nodes*, ou nós.

Para Santos (2018) uma das vantagens dessa arquitetura é o fato de ela ser ideal para dividir tarefas e cargas de trabalho entre nós. Nesse sentido, Barcellos e Gaspary (2006) apresentam outras três razões que tornam esse modelo de redes atrativo. As redes P2P possuem uma alta escalabilidade e podem lidar bem com grandes e pequenos grupos de participantes. Além disso, como esse tipo de rede não possui uma entidade central, elas podem oferecer mais estabilidade nas aplicações, já que elas resistem melhor a ataques de negação de serviço, por exemplo. Outro ponto importante é o fato de as redes P2P oferecerem uma autonomia aos participantes, já que eles participam da rede de acordo com seu interesse e disponibilidade, podendo assim, tomar suas decisões sem depender de outras entidades.

Colaborando com a discussão, Rocha et al. (2004) afirmam que a não existência um servidor central, simplifica a formação da rede, já que não é necessário investir em hardware de alto desempenho. Além disso, as redes P2P possibilitam a utilização do processamento e armazenamento subutilizado em dispositivos ociosos.

3.3 Criptomoedas

Este capítulo introduz o conceito de criptomoedas e demais definições relacionadas ao tema. Em seguida, apresenta uma breve contextualização do seu surgimento, enfatizando o Bitcoin e o Ethereum, respectivamente.

3.3.1 Definição

Segundo Silva e Machado (2017), as moedas digitais surgiram no cenário de jogos de computador e redes sociais, contudo ao decorrer do tempo, passaram a ser usadas em transações

financeiras no mundo real.

De acordo com Baptista (2019), em economia, moeda é um meio usado para o pagamento de bens e serviços ou quitação de dívidas. Dessa forma, uma moeda possui três funções na economia:

- **Meio de pagamento**: a possibilidade de o dinheiro ser globalmente reconhecido como meio de troca no comércio de bens e serviços de uma determinada região.
- **Reserva de valor**: as pessoas estarem propensas a reter a sua riqueza acumulada em moeda acreditando que a mesma não irá sofrer grande redução de valor.
- **Unidade de conta**: os bens e serviços estão cotados na unidade monetária dessa moeda.

Nesse sentido, dentre essas funções, meio de pagamento é a mais importante, já que ela possui as outras duas funções como derivadas e distingue a moeda dos demais ativos financeiros. (BAPTISTA, 2019).

Para Baptista (2019), existem três tipos de moedas virtuais:

1. **Moedas virtuais fechadas**: moedas que praticamente não estão ligadas a economia real, utilizadas normalmente em jogos. Elas são obtidas pelos jogadores de acordo com o seu desempenho, portanto, são limitadas a compras no ambiente do jogo.
2. **Moedas virtuais de fluxo unidirecional**: moedas que podem ser compradas usando dinheiro real e que não podem ser trocadas de volta para a moeda original. Assim, elas podem ser usadas na compra de bens e serviços virtuais ou reais.
3. **Moedas virtuais de fluxo bidirecional**: moedas que podem ser compradas e vendidas de acordo com a taxa de câmbio vigente. Esse tipo de moeda é idêntica a uma moeda real, permitindo compra de bens e serviços reais e virtuais.

Criptomoedas como o Bitcoin e Ethreum são moedas virtuais, as mesmas funcionam como meio de troca e não possuem todos os atributos das moedas reais. As moedas virtuais são caracterizadas por serem uma espécie de dinheiro digital que não possui regulamentação, além de ser emitido e regido por seus programadores e usado por uma grupo virtual específico. Deste modo, as criptomoedas fazem parte do terceiro tipo (moedas virtuais de fluxo bidirecional) sendo compradas e vendidas no mercado e podendo servir como meio de troca para bens e serviços. (BAPTISTA, 2019).

3.3.2 Surgimento

A história das criptomoedas está diretamente relacionada a duas áreas de estudo, os sistemas distribuídos e os sistemas de dinheiro eletrônico. (BRANDÃO, 2020). Apesar de

possuírem poucas ligações no início, ambas as áreas possuem relação com os avanços da criptografia bem como estudos relacionados ao dinheiro eletrônico. Assim, conforme afirma Figueiredo (2020), a partir da década de 80, muitos pesquisadores começaram a buscar uma forma de desenvolver moedas digitais, isso aconteceu devido ao avanço em algumas áreas, em especial, a área da criptografia.

Figueiredo (2020) e Brandão (2020) relataram que em 1982 o cientista da computação e criptógrafo David Chaum, criou o conceito de assinaturas cegas, uma novidade em termos de criptografia que viria a possibilitar a criação de sistemas de pagamentos mais seguros, não rastreáveis, mais auditáveis, com mais controle e com maior privacidade quando comparados com os sistemas existentes na época.

A proposta de Chaum girava em torno de um caixa digital que possibilita aos usuários usarem a moeda digital de tal forma que os gastos não fossem rastreáveis pela outra parte. A partir desta tecnologia, Chaum criou o eCash, um sistema criptográfico de dinheiro digital que possuía como característica o anonimato. Apesar disso, o eCash não teve muita aceitação o que fez com que David Chaum vendesse suas patentes em 1998. (FIGUEIREDO, 2020; BRANDÃO, 2020).

Segundo Figueiredo (2020) e Brandão (2020) além do eCash, foram criadas diversas moedas digitais e sistemas de pagamentos virtuais antes do Bitcoin (considerada a primeira criptomoeda). Porém, por funcionarem de forma centralizada estas iniciativas acabaram não avançando, devido a fraudes e intervenções governamentais.

Outro projeto importante que surgiu antes do Bitcoin foi o B-money. Ele utilizava o conceito de *Proof-of-work* ou prova de trabalho que, como será explicado posteriormente na seção 4.1.7, é uma parte fundamental do protocolo Bitcoin. Além disso, o B-money é uma referência usada no próprio *whitepaper* do Bitcoin. Outro projeto importante foi o Bit Gold, criado por Nick Szabo em 1998, se trata de uma plataforma monetária descentralizada e apontada como precursora do Bitcoin, além de ser uma das principais inspirações para criação do mesmo. (FIGUEIREDO, 2020).

De acordo com Brandão (2020), o movimento Cyberpunk que ganhou força em 1990, também inspirou a criação das moedas digitais. Eles pregavam a utilização da criptografia e métodos similares como meios para provocar mudanças sociais e políticas. Além disso, defendiam o uso de tecnologias de criptografia para dar maior privacidade para os usuários.

Outro fator que influenciou o surgimento do Bitcoin foi a crise econômica de 2008. O excesso de crédito disponibilizado pelos bancos colaborou para que a crise acontecesse, já que grande parte dos empréstimos aprovados por esses bancos, resultou no endividamento das pessoas e consequências negativas para economia como um todo. Assim, o Bitcoin surgiu como uma alternativa ao modelo econômico tradicional, onde se tem uma grande dependência de entidades responsáveis por intermediar e validar as transações. O artigo original do Bitcoin foi

publicado 45 dias após a eclosão da crise. (FIGUEIREDO, 2020; PEREIRA, 2022).

> O surgimento das criptomoedas se deve essencialmente ao descontentamento do sistema tradicional onde o Estado é detentor do monopólio da emissão da moeda. Também a desconfiança e descrença nas instituições financeiras que surgiram devido à falência de alguns bancos, então detentores de um prestígio e credibilidade considerada inabalável, contribuíram para o aparecimento e desenvolvimento da tecnologia Blockchain. (PEREIRA, 2022, p.42).

Dannen (2017) explica que as corporações gastam altas quantias de dinheiro construindo e mantendo serviços de software e TI para seus próprios funcionários e todas as suas linhas de negócios. Suas várias entradas e saídas são conciliadas por grandes bancos comerciais, que possuem arquitetura, política, base de código, bancos de dados e camadas de infraestrutura. Dessa forma, essas entidades necessitam de recursos para se manterem, o que acaba por elevar os preços e taxas para os consumidores. Já em um sistema bancário baseado em criptomoedas, todos os usuários (sejam empresas ou clientes) têm acesso direto ao mesmo sistema sem custo, com capacidade de programar transações. Uma vez que, o protocolo é gratuito e de código aberto, qualquer pessoa pode ativar um nó e se conectar na rede.

É interessante notar que antes da primeira criptomoeda descentralizada (Bitcoin) surgir, foram apontados vários conceitos que melhoraram a ideia original de David Chaum. Porém, apesar desses conceitos apresentarem melhorias incrementais, eles ainda possuíam elementos centralizados, logo, não se qualificavam como moedas completamente descentralizadas. (BRANDÃO, 2020).

3.3.2.1 Bitcoin

De acordo com Baptista (2019) e Silva e Machado (2017) a evolução nas áreas de criptografia, sistemas distribuídos e dinheiro eletrônico culminou no lançamento do artigo científico de Satoshi Nakamoto, publicado em 2008 na lista de discussão *The Cryptography Mailing List* , descrevendo seu protocolo e explicando de uma forma geral o funcionamento de um sistema que se viria a tornar o Bitcoin.

> O título do documento publicado por Satoshi foi *"Bitcoin: A Peer-to-Peer Electronic Cash System"* (que pode ser traduzido para algo como "Bitcoin: Um sistema par-a-par de dinheiro eletrônico"). É interessante ressaltar que o termo *cash* em inglês é usado para dinheiro em espécie, que é o conceito que o Bitcoin estava tentando recriar no mundo digital: quem possui *bitcoins*, a moeda do sistema, pode gastá-los trocando por produtos ou serviços sem precisar se identificar e informar dados pessoais, como é o caso das compras virtuais utilizando-se cartões de crédito. (FIGUEIREDO, 2020, p.9).

Dessa forma, em 2009 foi criada a rede Bitcoin com a emissão das primeiras moedas e usando uma implementação baseada no artigo de Satoshi Nakamoto e em 2010. O valor inicial foi definido por pessoas no fórum BitcoinTalk. (FIGUEIREDO, 2020; SILVA; MACHADO, 2017).

Segundo Figueiredo (2020), alguns fatos importantes que ocorreram nos primeiros anos após a criação do Bitcoin são:

- A primeira transação de *bitcoins* foi de 10 BTC para o programador Hal Finney.
- O primeiro registro de compra com Bitcoin: 2 pizzas por 10.000 BTC, em 17 de maio de 2010, por Laszlo Hanyecz.
- Em 15 de agosto de 2010, uma falha de segurança foi explorada para gerar mais de 184 bilhões de *bitcoins* indevidamente, porém foi corrigida e o protocolo foi atualizado.

3.3.2.2 Ethereum

De acordo com Antonopoulos e Wood (2018), o Ethereum surgiu em um momento em que as pessoas reconheciam o poder do modelo Bitcoin e estavam tentando ir além em relação as aplicações das criptomoedas. Entretanto, os desenvolvedores enfrentavam um dilema: eles precisavam construir a partir do Bitcoin ou construir uma nova Blockchain.

Construir sobre o Bitcoin significava viver dentro das restrições da rede e tentar encontrar soluções alternativas. O conjunto limitado de tipos de transações, tipos de dados e tamanhos de armazenamento de dados parecia limitar os tipos de aplicativos que podiam ser executados diretamente no Bitcoin; qualquer outra coisa precisava de camadas adicionais, e isso imediatamente negou muitas das vantagens de usar uma Blockchain pública. Para projetos que precisavam de mais liberdade e flexibilidade enquanto permaneciam na cadeia, uma nova Blockchain era a única opção. Mas isso significava muito trabalho: inicializar todos os elementos de infraestrutura, testes exaustivos etc. (ANTONOPOULOS; WOOD, 2018).

Segundo Buterin (2017) e Antonopoulos e Wood (2018), no final de 2013, Vitalik Buterin, um jovem programador e entusiasta do Bitcoin, começou a pensar em ampliar ainda mais as capacidades do Bitcoin e do Mastercoin (um protocolo estendeu o Bitcoin para oferecer contratos inteligentes rudimentares). Em outubro daquele ano, Vitalik propôs uma abordagem mais generalizada para a equipe Mastercoin, que permitiu contratos flexíveis e programáveis (mas não Turing-completos[1]) para substituir a linguagem de contratos especializada da Mastercoin. Apesar da equipe da Mastercoin ficar impressionada, esta proposta era uma mudança radical demais para se encaixar no roteiro de desenvolvimento da equipe.

Dessa forma, Vitalik começou a desenvolver e expandir sua ideia, até que em dezembro de 2013, ele compartilhou um *whitepaper* que descrevia o conceito por trás do Ethereum: uma Blockchain Turing completa e de uso geral. Assim, algumas dezenas de pessoas viram este rascunho inicial e ofereceram *feedback*, ajudando Vitalik evoluir a proposta. O Dr. Gavin Wood, no entanto, foi uma das primeiras pessoas a entrar em contato com Vitalik e se oferecer para

[1] Dizer que algo é Turing completo, significa dizer que ele pode computar qualquer algoritmo que possa ser computado por uma máquina de Turing, dadas as limitações de memória finita. (ANTONOPOULOS; WOOD, 2018)

ajudar com suas habilidades de programação em C++. Assim, Gavin se tornou Cofundador, codesigner e CTO da Ethereum. (BUTERIN, 2017; ANTONOPOULOS; WOOD, 2018).

A partir de dezembro de 2013, Vitalik e Gavin refinaram e desenvolveram a ideia juntos, construindo a camada de protocolo que se tornou o Ethereum. Assim, eles trabalharam durante anos e em 30 de julho de 2015, o primeiro bloco Ethereum foi minerado. (ANTONOPOULOS; WOOD, 2018).

3.3.3 Carteiras

O termo ”carteira” pode ser usado para se referir a coisas diferentes no universo das criptomoedas. Em um nível mais alto, a carteira pode ser considerada uma aplicação como uma interface de uso primária para o usuário, neste caso, ela controla o acesso ao ativos do usuário, gerencia suas chaves e endereços, acompanha o balanço, cria e assina transações. Porém, de outra perspectiva, a carteira pode ser vista como cada conta criada para realizar transações em uma criptomoeda. (ANTONOPOULOS, 2019).

De acordo com Rodrigues (2016) e Antonopoulos e Wood (2018), do ponto de vista de um programador, a palavra carteira se refere a um sistema usado para armazenar e gerenciar as chaves do usuário. Assim, toda carteira possui um componente responsável por gerenciar as chaves. Atualmente existem três tecnologias de carteira:

- A primeira versão (não-determinística), onde se tem um conjunto de chaves privadas aleatórias e pode-se gerar mais chaves posteriormente. Neste caso, cada chave é gerada de forma independente a partir de um número aleatório diferente. Assim, as chaves não são relacionadas entre si. O backup é custoso já que deve-se fazer uma cópia de cada nova chave privada gerada.

- A versão determinística, onde se tem um conjunto de chaves privadas geradas a partir de uma única chave mestra, conhecida como semente. Neste caso, faz-se o backup da semente, já que todas as chaves deste tipo de carteira estão relacionadas entre si e podem ser geradas novamente a partir da semente original.

- A versão determinística hierárquica e mnemônica, que visa tornar as carteiras determinísticas um pouco mais seguras contra perda de dados acidental. Onde se tem uma técnica refinada de geração de chaves a partir de uma semente. Neste caso, a semente é codificada em um formato literal, como uma lista de 12 ou 24 palavras para serem usadas em caso de acidente. Estas são conhecidas como as palavras de código mnemônico da carteira.

Uma consideração importante ao projetar carteiras é equilibrar conveniência e privacidade. A carteira Ethereum mais conveniente é aquela com uma única chave e endereço que você reutiliza para tudo. Infelizmente, tal solução é um pesadelo de privacidade, pois qualquer pessoa

pode facilmente rastrear e correlacionar todas as suas transações. Usar uma nova chave para cada transação é melhor para privacidade,mas se torna muito difícil de gerir. O equilíbrio correto é difícil de alcançar, por isso que um bom design de carteira é fundamental. (ANTONOPOULOS; WOOD, 2018).

3.3.4 Mineração

A mineração pode ser entendida como uma troca entre os mineradores e a Blockchain, visto que os mineradores emprestam poder computacional ao sistema para realizar as validações das transações e, como recompensa, eles ganham criptomoedas por esse serviço. Esse processo de emissão de novas criptomoedas é chamado de mineração, pois o gasto de energia e poder computacional em troca das moedas é análogo a atividade de mineradores de ouro gastando seus recursos e tempo para adicionar mais ouro em circulação. (SICHEL; CALIXTO, 2018; FIGUEIREDO, 2020).

Em outras palavras, mineração no contexto do Bitcoin, é o nome dado ao processo onde se usa o poder computacional para nomear um bloco como um bloco canônico mais recente na cadeia. Assim, a mineração atinge o consenso requerido para tornar válidas as mudanças de estado, e os mineradores são pagos por contribuir com a construção desse consenso. (DANNEN, 2017).

Assim, para Antonopoulos e Wood (2018), o objetivo real da mineração (e de todos os outros modelos de consenso) é proteger a Blockchain, mantendo o controle sobre o sistema descentralizado e difundido pelo maior número possível de participantes. Dessa forma, a recompensa da moeda recém-cunhada é um incentivo para aqueles que contribuem para a segurança do sistema: um meio para um fim. Nesse sentido, a recompensa é o meio e a segurança descentralizada é o fim.

4 Funcionamento das criptomoedas

Este capítulo apresenta como funcionam as criptomoedas, em particular, o Bitcoin e Ethereum; e faz uma discussão a respeito de suas diferenças técnicas e as implicações disso.

4.1 Bitcoin

Conforme explicado por Nakamoto (2008) no artigo que propôs o Bitcoin (*whitepaper*), o modelo tradicional de pagamento depende fortemente de entidades financeiras para processar transações de forma confiável. Nesse modelo surge a necessidade de se estabelecer confiança nessas entidades, o que pode representar um problema na visão de algumas pessoas. Outro ponto criticado nesse modelo é o fato de existir um custo para mediação dos conflitos por parte das entidades, o que impacta diretamente o custo das transações.

Dessa forma, segundo Nakamoto (2008) o Bitcoin surge como um método de pagamento alternativo baseado em prova criptográfica em vez de confiança, no qual, reverter as transações é impraticável, pois seria necessário quebrar a criptografia utilizada nas transações. Além disso, o problema do gasto duplo, que pode acontecer em sistema de pagamento baseado em moeda digital, é resolvido usando um mecanismo de consenso. Para fraudar esse sistema seria necessário que uma entidade controlasse a maioria absoluta do poder computacional utilizado na rede.

4.1.1 Blockchain

Segundo Sichel e Calixto (2018) o livro contábil da Blockchain, se trata de um banco de dados de contabilidade pública que registra as transações da criptomoeda Bitcoin. Além disso, como explicado por Baptista (2019), as transações são validadas por uma rede de computadores e as informações dessas transações são guardadas em blocos, e é daí que surge o nome dessa tecnologia, ”Blockchain”.

Nesse sentido, Santos (2018) explica que a tecnologia Blockchain segue os moldes das redes *peer-to-peer* e surgiu com os objetivos de descentralizar o armazenamento de dados e oferecer maior transparência às transações efetuadas, além de utilizar conceitos e paradigmas da Segurança da Informação.

A tecnologia Blockchain foi definida em um artigo publicado em 2008, assinado pelo pseudônimo Satoshi Nakamoto. A seguir, veremos mais detalhes a respeito de seu funcionamento e de como ela se utiliza dos conceitos inciais apresentados anteriormente.

4.1.2 Nós da rede

Assim como Figueiredo (2020) apresenta, o Bitcoin está estruturado como uma rede *peer-to-peer* sobre a internet, logo, os usuários da rede são pares entre si e são chamados de nós. Um nó da rede Bitcoin pode executar outras funções além do protocolo P2P. Essas funções são: carteira, mineração, Blockchain completa e roteamento. Um exemplo de nó completo e das funções executadas por ele pode ser visto na Figura 4.

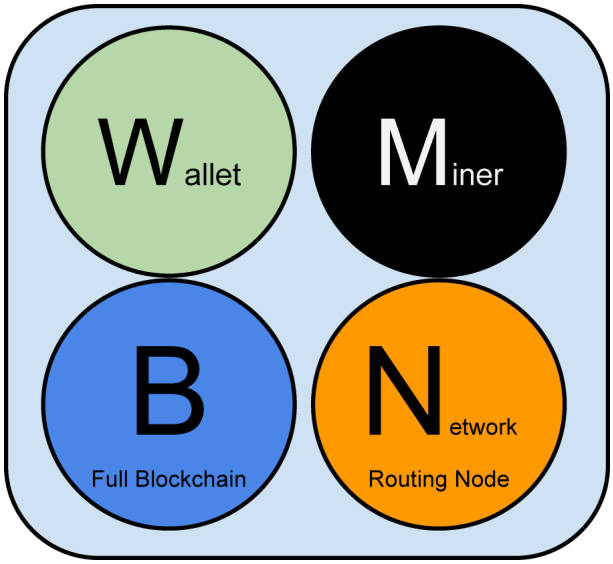

Figura 4 – Nó completo e suas funções (ANTONOPOULOS, 2019)

Todos os nós incluem a função de roteamento para participar da rede e podem incluir outras funcionalidades. A função de roteamento é representada pela círculo laranja na Figura 4. (ANTONOPOULOS, 2019).

Dessa forma, segundo Antonopoulos (2019) alguns nós são capazes de manter uma cópia completa e atualizada da Blockchain. Estes são chamados de nós completos. Eles podem, de forma autônoma, verificar transações sem a interferência externa. Já os SPV, ou *Simplified Payment Verification*, conforme explicado por Figueiredo (2020) são nós que possuem uma cópia parcial da Blockchain, eles não validam todas as regras do consenso e necessitam da conexão com um nó completo para se comunicar com a rede e verificar transações.

Os nós que possuem a função de mineração, competem para criar novos blocos conforme será explicado na seção 4.1.7. Alguns nós de mineração também são nós completos e mantém uma cópia completa da Blockchain, enquanto outros são SPV e necessitam se conectar a um nó completo. Assim, a função de mineração é representada pela círculo preto na Figura 4.

As carteiras também podem ser parte de um nó completo, porém muitas funcionam como nós SPV. (ANTONOPOULOS, 2019). A função de carteira é representada pela círculo verde na Figura 4.

A rede Bitcoin é composta por nós que executam o protocolo P2P Bitcoin. No entanto, os nós também executam outros protocolos especializados, nos referimos à esse rede mais ampla

como rede Bitcoin estendida. (ANTONOPOULOS, 2019). Ligados a rede principal do Bitcoin, existem servidores de pool e *gateways* que conectam nós executando outros protocolos, como o *Stratum Protocol* (usados para realizar a mineração em conjunto como será detalhado na seção 4.1.7). A Figura 5 apresenta alguns tipos de nós presentes na rede Bitcoin:

Figura 5 – Tipos de nós na rede Bitcoin. Adaptada de Antonopoulos (2019)

A Figura 6 mostra a rede Bitcoin estendida com vários tipos de nós, bem como servidores, roteadores, clientes de carteira e outros protocolos usados pelos nós para comunicarem entre si.

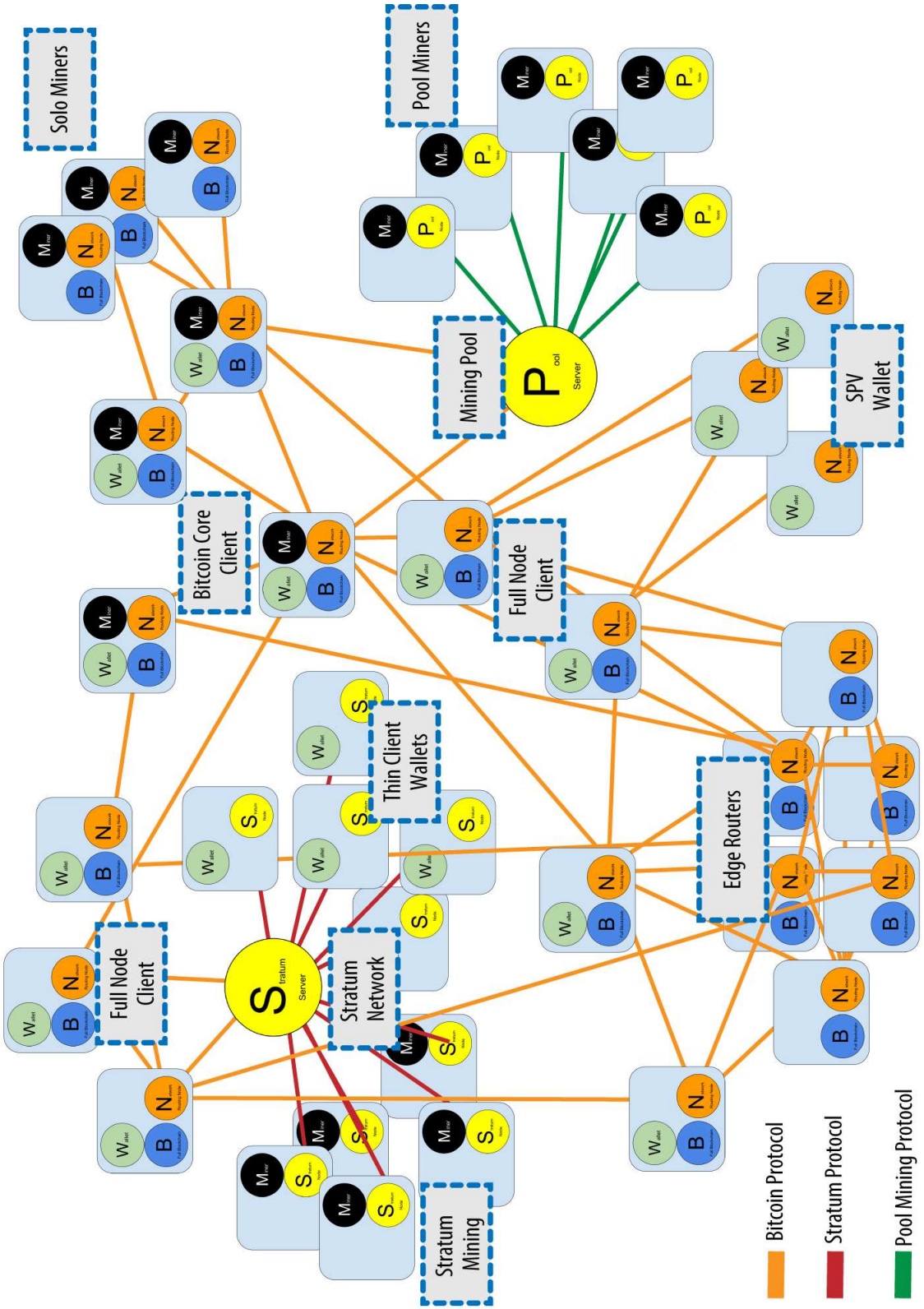

Figura 6 – Rede do Bitcoin estendida (ANTONOPOULOS, 2019)

Logo, como mostra a Figura 6 os vários tipos de nós, se comunicando através do

protocolo Bitcoin (em laranja), Stratum (em vermelho) ou protocolos de *pool* de mineração (em verde) formam a rede estendida do Bitcoin.

4.1.3 Endereços

Segundo Figueiredo (2020) o endereço de uma carteira do Bitcoin é um número baseado na chave privada usada para assinar as transações digitalmente. Uma chave privada K nada mais é do que um grande número aleatório. A partir dessa chave, calcula-se uma chave pública k, usando multiplicação de curvas elípticas. Para gerar o endereço Bitcoin, primeiro, deve-se calcular o *hash* SHA256 da chave privada k e finalmente, calcula-se o *hash* RIPEMD160 do resultado obtido no passo anterior. Conforme explica Rodrigues (2016), esse endereço é codificado em uma string alfanumérica usando Base58Check e começa com o dígito 1 ou 3. Um ponto interessante é que um usuário pode gerar vários endereços para si. Essa é uma pratica bem comum.

A Figura 7 mostra o esquema de criação de um endereço de carteira do Bitcoin a partir da chave pública.

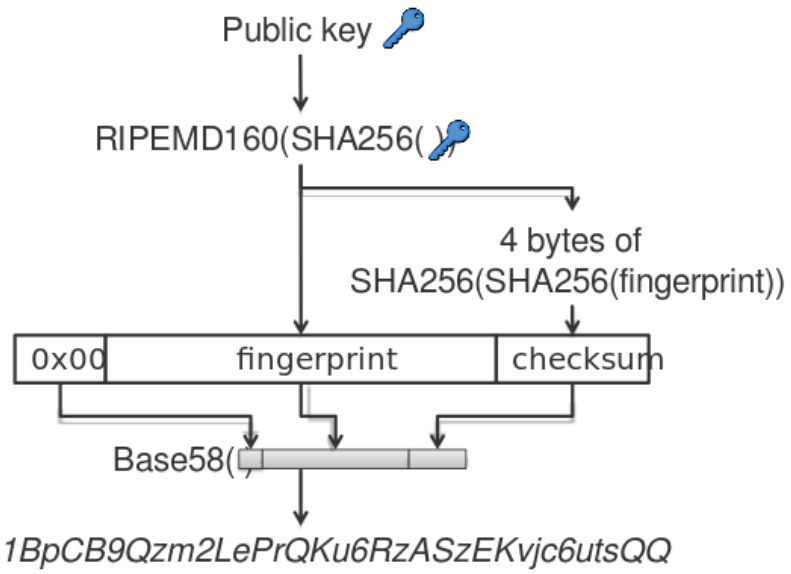

Figura 7 – Endereço Bitcoin (WANDER, 2013a)

Na Figura 7 é possível observar todo o processo de geração de um endereço. Onde o mesmo é gerado usando um *hash* da chave pública e codificado usando Base58Check.

4.1.4 Carteiras

Conforme explicado por Figueiredo (2020) e Baptista (2019) a carteira é identificada por um endereço que deve ser informado nas transações. As transações então, devem ser assinadas digitalmente com a chave privada correspondente, assim o emissor comprova que é o detentor daquela carteira.

A função *hash* é utilizada na criação das carteiras, para gerar o endereço Bitcoin. Através da chave pública não se consegue chegar à chave privada do utilizador. O endereço serve como o número de conta ou IBAN, identificando quem tem a propriedade dos *bitcoins*, e em caso de transferência quem é o emissor e receptor da transação. A chave privada é o equivalente a uma senha e é utilizada para gerar a assinatura digital necessária nas transações, pois, ela assegura a propriedade de determinado endereço pelo emissor da transação. (BAPTISTA, 2019).

Segundo Rodrigues (2016), uma carteira não necessita ser um nó completo na rede, ela pode operar de maneira mais leve, consultando apenas blocos de seu interesse para verificar suas transações. Porém, Figueiredo (2020) adverte que é mais seguro executar a carteira em um nó completo da rede e caso não seja possível, deve-se buscar um nó completo confiável para se conectar.

Para Figueiredo (2020), a segurança das carteiras envolve manter a chave privada em sigilo. Assim, a mesma deve ser guardada em um local seguro e com cautela, já que a perda ou esquecimento da chave pode causar a impossibilidade de realizar transações com as criptomoedas. Na prática, o detentor de uma carteira não possui moedas, mas sim chaves privadas que geram as chaves públicas cujos endereços estão registrados na Blockchain, e que por consequência possuem uma soma de valores atribuídos a eles. De maneira simplificada, dizer que alguém possui 1 Bitcoin significa dizer que: a rede consente que o detentor de tais endereços possui 1 Bitcoin (RODRIGUES, 2016, p. 11).

4.1.5 Transações

De acordo com Figueiredo (2020), as transações se tratam da transferência de *bitcoins* entre endereços. Essas transações são feitas a partir de mensagens usando a assinatura digital criada com a chave privada do emissor e destinadas a rede Bitcoin. Conforme explicado por Antonopoulos (2019) as transações são a forma que um usuário da rede tem de comunicar aos demais usuários que um certo valor em Bitcoin está sendo transferido e terá um novo dono.

Figueiredo (2020) explica que as transações são feitas utilizando as carteiras e são transmitidas a rede usando um nó completo ou um nó leve conectado a um nó completo como explicado anteriormente. Assim, as transações transmitidas são reunidas pelos mineradores em blocos, que posteriormente são gravados permanentemente na Blockchain. Isso permite que as transações sejam irreversíveis, ou seja, uma vez que uma transação é aceita na Blockchain não é possível revertê-la. (RODRIGUES, 2016).

Além disso, Rodrigues (2016) e Figueiredo (2020) explicam que as transações são compostas dos endereços de entrada e saída, onde mais de um endereço pode compor a entrada e mais de um endereço pode compor a saída. As entradas representam os débitos e as saídas, créditos em endereços Bitcoin. E sendo, o valor total da saída menor ou igual ao valor total da entrada, tendo a diferença dada como taxa de transação para o minerador que incorporar a transação em seu bloco. Além disso, as transações contam com a assinatura digital dos donos em cada entrada, que pode ser validada por qualquer um na rede. (ANTONOPOULOS, 2019).

A Figura 8 apresenta dois exemplos de transações.

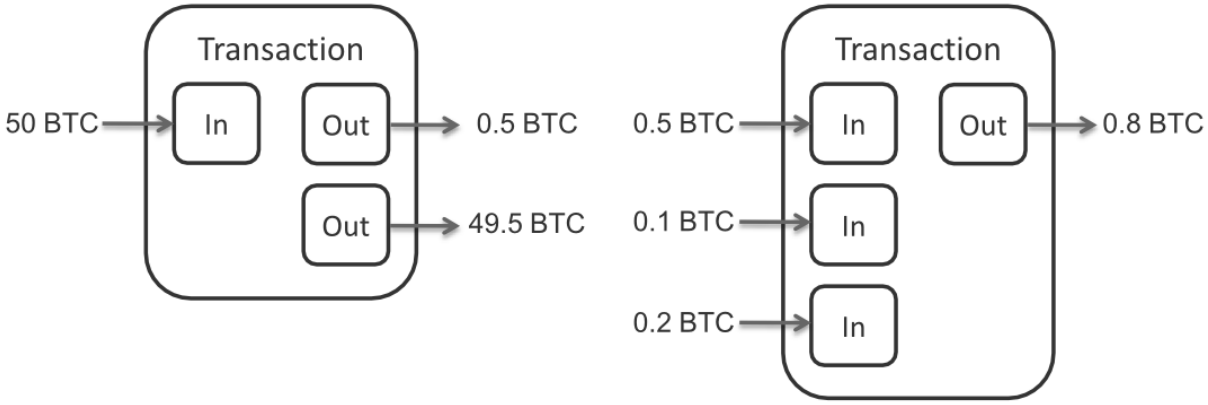

Figura 8 – Transações no Bitcoin: entradas e saídas (WANDER, 2013c)

Na Figura 8 é possível observar uma transação com uma entrada de 50 BTC e duas saídas de 0.5 e 49.5 BTC, respectivamente, uma outra transação com três entradas de 0.5, 0.1 e 0.2 BTC, respectivamente, e uma saída de 0.8 BTC. Pode-se observar que as entradas e saídas nas transações podem ser divididas e atribuídas à diferentes endereços.

As transações em uma Blockchain formam uma cadeia, onde a entrada da transação atual faz uma referência as saídas das transações anteriores que geraram o respectivo saldo. Além disso, com a identificação de transação de origem é possível ter acesso às transações anteriores, para certificar que o emissor possui a quantia a ser transferida. Da mesma forma, quando o receptor for utilizar a quantia recebida dessa transação em outra, ele também deve informar a transação que comprova a origem do saldo. (ANTONOPOULOS, 2019).

Figueiredo (2020) explica ainda, que para que haja uma transação é preciso:

- Chave pública do emissor.
- Chave privada do emissor para assinar a transação.
- Chave pública como endereço de destino.

Porém, o usuário só precisa informar o endereço de destino, caso utilize um software de carteira.

Todos esses itens e a cadeia de transações, bem como as assinaturas, são ilustradas na Figura 9.

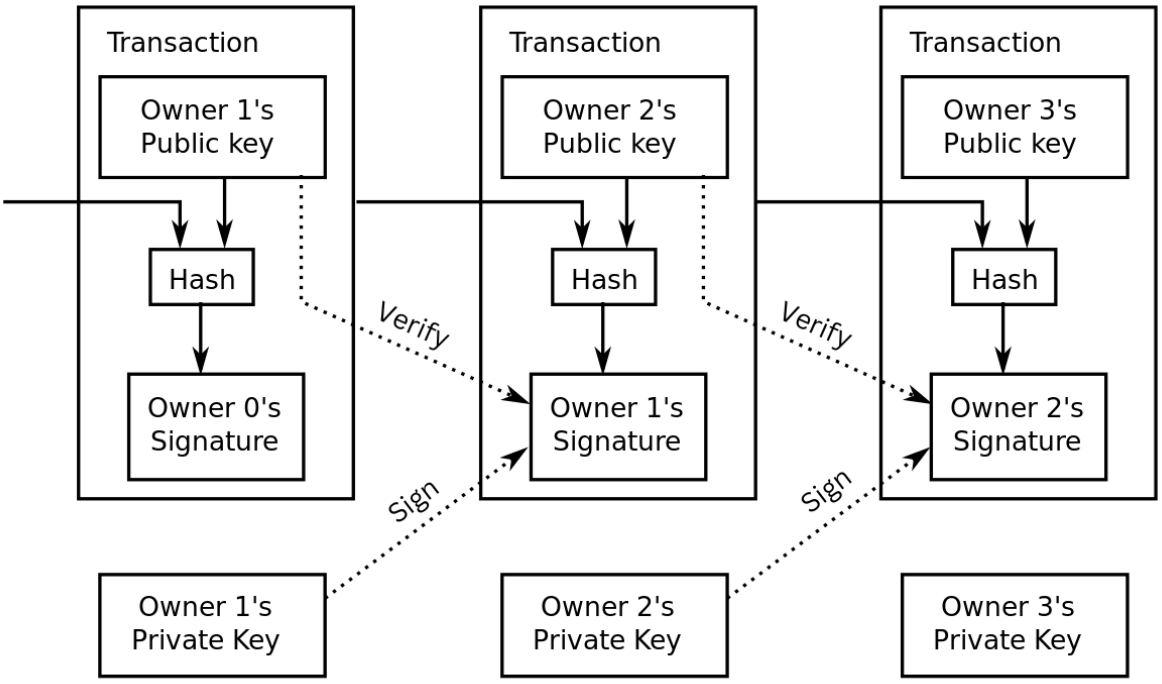

Figura 9 – Cadeia de transações. Adaptada de (NAKAMOTO, 2008)

A Figura 9 apresenta três transações. Cada uma dessas transações contém a chave pública do destinatário da transação, uma *hash* e a assinatura digital do usuário que realizou a transação. Sendo que, a *hash* é um resumo da transação anterior e da chave pública do destinatário, presente na transação atual.

> Apesar da limitação do número máximo de Bitcoin em circulação, este limite não cria um problema à sua utilização como moeda, uma vez que o Bitcoin permite operar até à oitava casa decimal 0,00000001, o que possibilita fazer-se transferências de baixo valor independentemente do preço do Bitcoin. À unidade mínima de transação dá-se o nome de satoshi, um Bitcoin vale 100 milhões de satoshi. O sistema para não trabalhar com casas decimais, trabalha sempre com satoshis, apesar de o normal ser o utilizador definir o valor a transferir em *bitcoins* (BAPTISTA, 2019, p. 19).

Como apresentado por Antonopoulos (2019), muitas transações no Bitcoin contam com as saídas compostas pelo endereço da pessoa que está sendo paga e também de quem está efetuando o pagamento. Isso acontece porque os valores recebidos nas transações anteriores (as saídas) são usados para compor as entradas das novas transações e eles não podem ser divididos. Logo, se um usuário recebeu 20 BTC em uma transação anterior e quer realizar uma transação no valor de 5 BTC, ele deve criar uma transação cuja entrada são os 20 BTC e duas saídas, uma de 5 BTC para o endereço de outro usuário e uma de 15 BTC para um endereço dele, isso desconsiderando a taxa de transação.

4.1.6 Blocos

Segundo Figueiredo (2020) os dados das transações feitas com *bitcoins* são gravados em blocos, esses blocos são organizados de forma linear. A essa organização se dá o nome de Blockchain, ou "Cadeia de blocos" e conforme Baptista (2019) explica que cada bloco de dados na cadeia aponta para um bloco anterior, que pode ser chamado de bloco pai. Dessa forma, novos blocos são sempre adicionados no fim da cadeia. É possível observar essa organização na Figura 10:

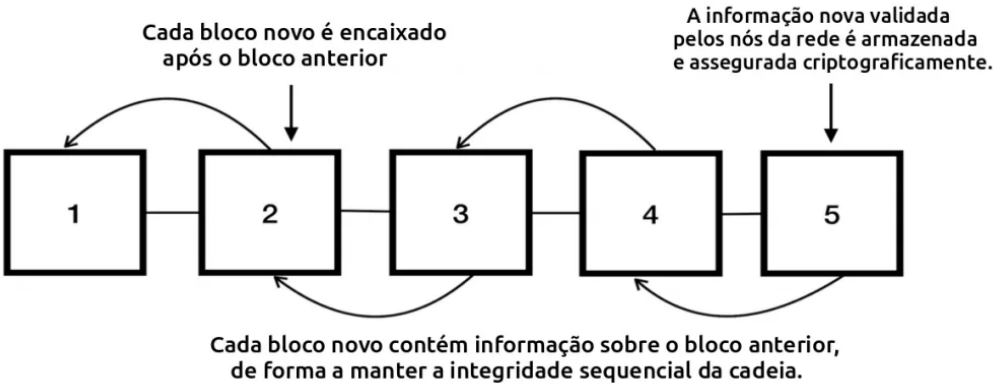

Figura 10 – Organização da cadeia de blocos (Blockchain). (LIMA, 2020)

A Figura 10 apresenta cinco blocos na Blockchain, cada um deles é encaixado e aponta para o bloco anterior. Exemplo, o bloco 5 aponta para o bloco 4, logo, o bloco 4 é pai do bloco 5.

Como Figueiredo (2020) explica, a cadeia de blocos é visualizada como uma pilha vertical onde os termos "block height" e "block depth" são usados. Block height se refere a altura de um bloco, ou seja, a distância de um bloco até o primeiro. Já Block depth é usado para definir a profundidade, ou seja, quantos blocos foram adicionados depois daquele na cadeia, contando os filhos diretos e indiretos.

Conforme Baptista (2019) e Figueiredo (2020), cada bloco é composto por um conjunto de transações que são propagadas na rede e coletadas pelos mineradores. Essas transações são organizados utilizando uma estrutura de dados do tipo árvore denominada *Merkle Tree*.

*Merkle Tree*s, ou árvores de dispersão, são árvores nas quais cada nó folha (elemento sem ramos) possui o *hash* de um bloco de dados, e onde cada nó que não é folha (elemento com ramos) possui o *hash* criptografado de seus nós filhos. *Merkle Trees* são consideradas como solução adequada para a verificação eficiente e segura de conteúdo em grandes quantidades de dados (SANTOS, 2018, p. 21). A estrutura de uma *Merkle Tree* pode ser vista na Figura 11, nela é possível observar também que cada nó possui um *hash* determinado de acordo com seus nós filhos.

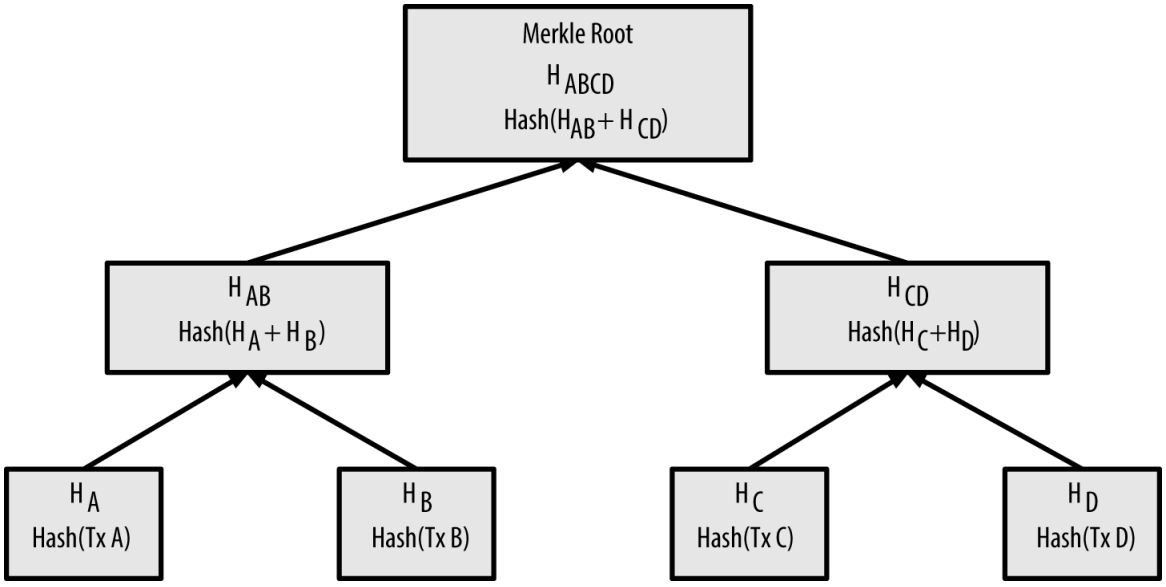

Figura 11 – Estrutura de uma Merkle Tree(ANTONOPOULOS, 2019)

A Figura 11 mostra um exemplo de uma Merkle Tree de um bloco com quatro transações.

O cabeçalho de um bloco possui dois *hashes* muito importantes: *hash* da raiz de Merkle do próprio bloco e *hash* do bloco anterior (que por sua vez possui o *hash* do bloco precedente e sua própria raiz). O uso de *hashes* ajuda a garantir a integridade dos dados, pois a alteração de uma transação em um bloco implica na mudança da *hash* do mesmo e de todos os blocos filhos.

As transações são organizadas nos blocos utilizando *Merkle Tree*s, onde no primeiro nível da árvore são dispostos os *hashes* de cada transação. Do segundo nível em diante, os *hashes* do nível anterior são concatenados dois a dois, e então computa-se o *hash* de cada par, assim, esse processo é seguido até o último nível, a raiz de Merkle. (FIGUEIREDO, 2020).

Conforme explicado por Antonopoulos (2019), um bloco é composto por: um campo que especifica o seu tamanho, um cabeçalho com as informações mais relevantes, um contador de transações e as transações do bloco. Essa estrutura está resumida na Tabela 1.

Campo	**Descrição**	**Tamanho**
Tamanho do bloco	O tamanho do bloco em bytes	4 bytes
Cabeçalho do bloco	Informações importantes compõem o cabeçalho do bloco	80 bytes
Contador de transações	Quantas transações fazem parte do bloco	1-9 bytes (VarInt)
Transações	As transações presentes no bloco	Tamanho variável

Tabela 1 – Estrutura do bloco

O cabeçalho do bloco é composto por: um campo ”versão” que apresenta a versão do software/protocolo, uma referência ao bloco anterior, uma referência a árvore de transações presente no bloco, o tempo aproximado de criação do bloco, a dificuldade de geração do bloco e o *nonce*. Essa estrutura está resumida na Tabela 2. (ANTONOPOULOS, 2019).

Campo	Descrição	Tamanho
Versão	A versão do software/protocolo	4 bytes
hash do bloco anterior	Uma referência ao bloco anterior na cadeia (Bloco pai)	32 bytes
Árvore de Merkle	Uma referência para raiz da árvore de transações do bloco	32 bytes
Timestamp	O tempo de criação aproximado do bloco	4 bytes
Dificuldade de geração	A dificuldade de geração do bloco de acordo como o algoritmo *Proof-of-Work*	4 bytes
nonce	Um contador usado no algoritmo *Proof-of-Work*	4 bytes

Tabela 2 – Estrutura do cabeçalho de um bloco

Figueiredo (2020) explica que uma transação pertencente a um bloco válido na cadeia, possui uma confirmação. Cada bloco adicionado posteriormente ao bloco válido, é uma confirmação adicional. Assim, considera-se que quanto mais confirmações tem uma transação, menor é o risco de que ela seja invalidada, já que seria necessário mais esforço computacional para recalcular os blocos. Dessa forma, a cadeia de blocos é responsável pela imutabilidade dos dados contido nela. Além disso, como apresentado por Nakamoto (2008) verificar se uma transação é válida se torna um processo simples, já que basta para o usuário checar se a transação está ligada a um ramo da árvore Merkle de um bloco em sua cadeia. E desde que a sua cópia da cadeia seja longa o bastante, pode-se confirmar que a rede possui um consenso a respeito daquela transação.

> É interessante destacar que o primeiro bloco de uma Blockchain não é conectado a um bloco prévio e é conhecido como *"genesis block"*, definido inalteradamente, ou seja, *hardcoded* no código-fonte da Bitcoin, especificamente no arquivo chainparams.cpp. Na Blockchain da Bitcoin há, também, os blocos obsoletos, do inglês *stale blocks* e os órfãos, *orphaned* blocks. Os primeiros são assim classificados por serem minerados com sucesso, porém não entram na cadeia de blocos porque outros mineradores conseguiram adicionar blocos primeiro. Blocos órfãos (*orphaned* ou *detached blocks*) são blocos válidos que não possuem pai. Esse tipo de bloco podia ser criado em versões mais antigas do software Bitcoin Core, onde os nós da rede não validavam as informações dos pais do bloco antes de minerá-lo. (SANTOS, 2018, p. 30).

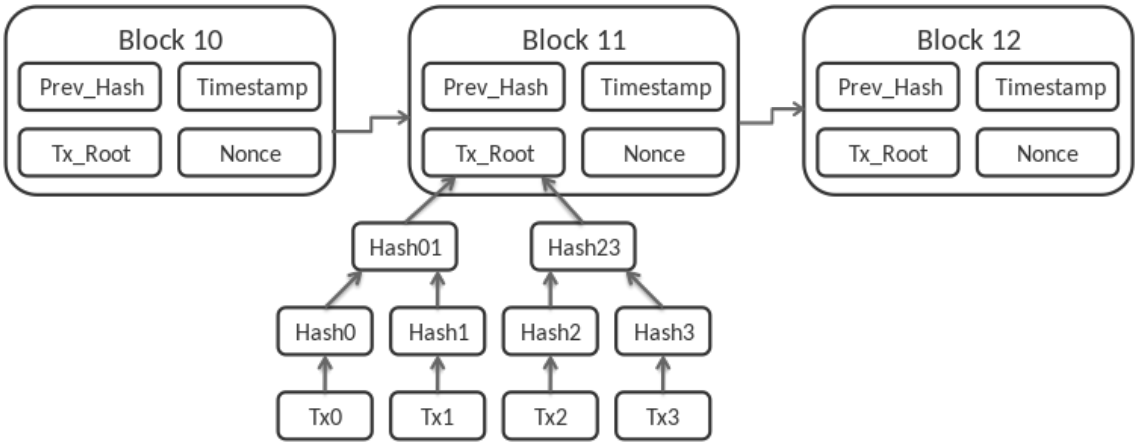

Figura 12 – Cadeia de blocos(WANDER, 2013b)

Na Figura 12 é possível observar a estrutura da cadeia de blocos e como eles estão interligados entre si.

4.1.7 Mineração

A forma como Bitcoin gera um consenso usando a rede descentralizada é a sua principal inovação. Esse consenso é feito de tal forma em que não existe uma votação e não é possível afirmar o momento exato em que ele acontece, logo, ele surge das interações entre os vários nós da rede, seguindo as regras pré-estabelecidas. Sendo toda a segurança da Blockchain é baseada nesse consenso. (FIGUEIREDO, 2020).

Segundo Figueiredo (2020), o consenso emerge de quatro processos independentes que ocorrem nos nós da rede Bitcoin:

- Verificação independente de cada transação pelos nós completos.
- Agregação das transações em novos blocos, de forma independente, pelos nós mineradores, junto com a prova-de-trabalho.
- Verificação independente dos novos blocos por cada nó e montagem da cadeia.
- Escolha independente feita em cada nó da cadeia, com maior esforço computacional demonstrado através da prova-de-trabalho.

Como explicado por Brochado (2018) e Baptista (2019) as transferências de *bitcoins* são processadas através da rede. Essa tarefa é executada pelos *miners* ou mineradores que trabalham de forma independente, agrupando as transações não confirmadas em novos blocos. Como existem vários mineradores, eles precisam resolver um problema matemático complexo para definir quem será o responsável por criar o novo bloco e adicioná-lo à cadeia de blocos (Blockchain). Aquele que conseguir resolver o problema primeiro, terá o direito de criar o novo bloco.

O desafio dos mineradores é alterar o *nonce* para encontrar um valor de *hash* para o cabeçalho menor que um determinado número (o que na prática implica que o *hash* deve começar com um determinado número de zeros à esquerda) (FIGUEIREDO, 2020, p. 22)). Assim, segundo Rodrigues (2016), os *miners* utilizam o seu poder computacional para tentar encontrar o *nonce* que satisfaça o valor de *hash* para o cabeçalho do bloco em que estão trabalhando e assim que o encontram, eles fazem o *broadcasting* desse bloco na rede. Logo, os outros mineradores podem facilmente verificar a legitimidade do bloco e então aceitá-lo, adicionando-o a sua cópia da Blockchain.

Devido a natureza da rede distribuída, pode ocorrer de dois ou mais nós encontrarem blocos válidos diferentes quase que simultaneamente. (FIGUEIREDO, 2020). Isso faz com que se tenha versões diferentes da cadeia por um tempo. Nesse caso, os nós da rede podem escolher qual das versões da cadeia eles irão considerar. Como Rodrigues (2016) explica, aceitar um bloco é o mesmo que confirmá-lo, e como já explicado anteriormente, após 6 confirmações pode-se considerar que o bloco faz parte de forma efetiva da Blockchain. Dessa forma, seguindo

o protocolo estabelecido, uma forma que os nós têm de resolver os conflitos na cadeia é sempre escolher a versão mais longa, que por consequência, possui mais confirmações.

Esse processo de validação, como explicado por Baptista (2019) é denominado "*proof-of-work*" ou prova de trabalho, onde para cada *miner* é difícil encontrar a solução do problema computacional proposto, mas quando o problema é resolvido, a verificação da solução é feita facilmente. Segundo Rodrigues (2016), o *proof-of-work* contribui para a segurança da rede, a medida que para fraudar um bloco é necessário que seja refeito o trabalho de reencontrar o *nonce* desse bloco, e fazer o mesmo para todos os seus filhos. No entanto, conforme a cadeia de blocos cresce e se espalha pela rede, o consenso é confirmado, tornando mais difícil a fraude. Em outras palavras, para fraudar um bloco, o atacante teria que fazer a prova de trabalho de todo o bloco e dos blocos posteriores, superando o trabalho feito dos nós honestos da rede. Em síntese, se o poder computacional em sua maioria provém de nós honestos, a cadeia honesta tende a crescer mais rápido, superando as demais. Dessa forma, o protocolo do Bitcoin incentiva o comportamento honesto dos mineradores. Uma vez que, é mais vantajoso participar da corrida por um bloco válido do que tentar fraudar transações. (FIGUEIREDO, 2020) e (NAKAMOTO, 2008).

O protocolo do Bitcoin foi construído de forma que existe um parâmetro de "dificuldade" que varia, de forma a manter o intervalo para encontrar um bloco válido em média 10 minutos. Dessa forma, à medida que o poder computacional da rede aumenta, a dificuldade para encontrar o *hash* que valida o bloco, também aumenta. Além disso, sempre que um bloco válido é adicionado a cadeia, a busca pelo *hash* válido recomeça. Logo, esse processo acaba sendo competitivo e demandando muito poder computacional e energia elétrica. (FIGUEIREDO, 2020).

Conforme apresentado por Figueiredo (2020), para motivar que os nós participem desse processo são oferecidas recompensas aos que encontram um bloco válido primeiro. Sendo que existem dois tipos de recompensa: pela criação do bloco e para cada transação incluída.

De acordo com Figueiredo (2020), a primeira transação no bloco é incluída pelo minerador e pode ser direcionado ao endereço de sua preferência. Se esse minerador encontra o bloco antes dos outros, ele recebe esses *bitcoins* que não são debitados de ninguém, são novos. Como explicado por Nakamoto (2008) isso incentiva os nós a apoiarem a rede como mineradores e é uma forma de colocar mais unidades da moeda em circulação, já que não existe uma entidade central para lidar com isso. Quando o Bitcoin entrou em funcionamento em 2009, essa recompensa era de 50 BTC, hoje ela é de 12,5 BTC. A cada 210.000 blocos o protocolo divide a recompensa pela metade, aproximadamente a cada 4 anos.

Portanto, uma transação pode conter a soma dos valores de saída, menor que a soma dos valores de entrada. Segundo Rodrigues (2016), essa diferença é dada como taxa para o minerador que incluir a transação em seu bloco.

> O protocolo de criação de nova moeda, estabelece que o Bitcoin tenha um volume máximo circulante de 21 milhões, que deverá ser atingido em 2140. Após essa data, não serão criados novos Bitcoin, passando os *miners* a serem recompensados apenas pelas comissões pagas por cada transação. Os utilizadores podem definir o montante da comissão a pagar. Valores de comissões mais elevados dão maior incentivo aos *miners* a processarem essa transferência de forma prioritária, face as outras transações em espera no *mempool* (BAPTISTA, 2019, p. 19).

Nesse sentido, Antonopoulos (2019) explica que a rede possui uma lista temporária de transações não confirmadas chamada de *memory pool* ou *mempool*. Para Baptista (2019), a *mempool* é necessária devido ao limite do número de transações possíveis em cada bloco, o protocolo do Bitcoin estabelece que o tamanho máximo do bloco é de 1 megabyte. Esse regra foi criada por razões técnicas, como a segurança da rede e questões práticas, como o uso em dispositivos com menos recursos.

Existem ainda, as *mining pools*, que são conjuntos de mineradores que reúnem poder de processamento em busca de receberem mais recompensas, uma vez que quanto maior o poder de processamento, maior a chance de minerar os blocos. Geralmente, as recompensas recebidas pela *mining pool* são distribuídas aos participantes com base nos ciclos de processamento que cada um utilizou durante o processo de mineração. (BAPTISTA, 2019).

4.1.8 *Forks*

As regras de consenso são a base para a colaboração entre todos os nós Bitcoin e são responsáveis pela convergência de todas as perspectivas locais em uma única Blockchain consistente em toda a rede. (ANTONOPOULOS, 2019). Entretanto essas regras podem variar no longo prazo. Já que, para evoluir e desenvolver o sistema de uma criptomoeda, as regras precisam mudar de tempos em tempos para acomodar novos recursos, melhorias ou correções de *bugs*. Ao contrário do desenvolvimento de software tradicional, no entanto, as atualizações para um sistema de consenso são muito mais difíceis e requerem coordenação entre todos os participantes.

De acordo com Antonopoulos (2019), quando ocorre uma mudança nas regras de consenso de uma criptomoeda, a rede da mesma pode se dividir em duas cadeias. Esse tipo de bifurcação é chamado de *hard fork*, porque após a bifurcação a rede não converge novamente em uma única cadeia. Em vez disso, as duas cadeias evoluem independentemente. Assim, *Hard forks* ocorrem quando parte da rede está operando sob um conjunto diferente de regras de consenso do que o resto da rede.

A Figura 13 mostra uma *Blockchain* com duas bifurcações:

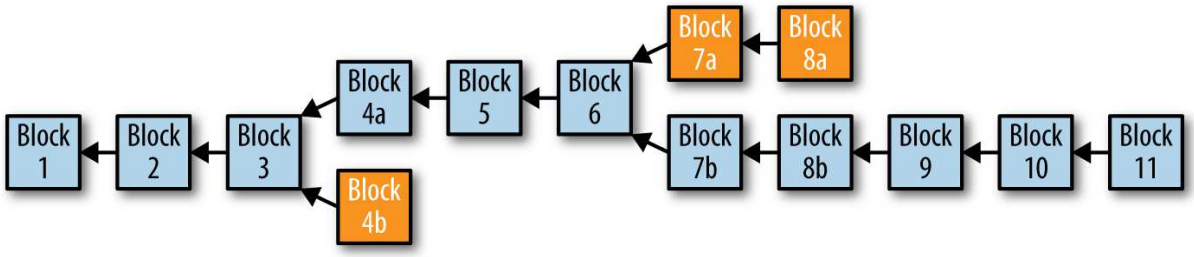

Figura 13 – *Hark Fork* (ANTONOPOULOS, 2019)

- Na altura do bloco 3, ocorre uma bifurcação de um bloco. Esse é o tipo de bifurcação espontânea em que duas partes da rede seguem dois ramos diferentes da cadeia por um curto período de tempo e após a mineração de um ou mais blocos a rede se reconverte e a bifurcação é resolvida (nesse caso a rede se reconverte com a mineração do bloco 5).
- Na altura do bloco 6, ocorre um *hard fork*. Isso significa que houve uma atualização das regras do consenso e à partir do bloco 7, mineradores que seguirem a atualização considerarão os blocos lançados pelos nós que não seguiram a atualização como inválidos (por não seguirem as regras de consenso), e vice-versa.

Nem todas as mudanças de regra de consenso causam um *hard fork*. Se a alteração for implementada de forma que um cliente não modificado ainda veja a transação ou o bloco como válido de acordo com as regras anteriores, a alteração pode ocorrer sem uma bifurcação. Desta forma, o termo *soft fork* foi introduzido para distinguir esse método de atualização de um "*hard fork*". Na prática, um *soft fork* é uma alteração compatível com as regras de consenso que permite que clientes não atualizados continuem a operar em consenso com as novas regras. (ANTONOPOULOS, 2019).

4.1.9 Altcoins

Antonopoulos (2019) apresenta que para desenvolvedores de software, o termo "*fork*" tem outro significado, confundindo o termo "*hard fork*". No software de código aberto, uma bifurcação ocorre quando um grupo de desenvolvedores escolhe seguir um roteiro de software diferente e inicia uma implementação concorrente de um projeto de código aberto.

Dessa forma, caso o *fork* de um projeto implemente uma mudança deliberada nas regras de consenso, ele irá preceder um *hard fork*. No entanto, para que esse tipo de *hard fork* ocorra, a nova implementação de software das regras de consenso deve ser desenvolvida, adotada e lançada. Portanto, quando isso acontece, essa nova implementação é considerada uma *altcoin*, já que ela é uma moeda alternativa a moeda original. (RODRIGUES, 2016) e (ANTONOPOULOS, 2019) .

Todavia, nestas ocasiões onde há a separação da Blockchain em duas moedas distintas, há uma grande flutuação de preços, pois, os usuários e a capitalização são divididos entre as duas moedas. Além do fato de que nesse caso, os mineradores se divergem na mineração das duas cadeias diferentes, sendo o poder de mineração dividido entre elas em qualquer proporção. O que pode representar uma grande queda no poder de mineração. (BAPTISTA, 2019) e (ANTONOPOULOS, 2019).

Para Rodrigues (2016) os principais motivos para a criação de uma *altcoin*, são:

- **Concorrência**: *altcoin* que possui o mesmo intuito da moeda original, mas o seu objetivo é competir com a ela. Neste caso, a *altcoin* pode dispor de algoritmos/parâmetros e/ou protocolos diferentes e pode implementar novas funcionalidades que a moeda original não possui.
- **Inovação**: *altcoin* que busca um novo objetivo/propósito com a tecnologia da moeda original.
- **Entretenimento, didática**: *altcoin* que possui o objetivo de oferecer o primeiro contato de usuários com as criptomoedas.
- **Golpe (*scam*)**: *altcoin* que é criada com o intuito de enganar pessoas, persuadindo-as a investir em uma moeda insegura e não explícita quanto a sua oferta monetária. Assim, seus autores acumulam uma grande quantia da moeda e lucram vendendo-a antes de sua queda.

De acordo com Figueiredo (2020) e Cavalcanti (2022), algumas das principais *altcoins* do Bitcoin são:

- Namecoin
  - Surgiu em abril de 2011.
  - Primeiro fork de código do Bitcoin conhecido.
  - O termo mais usado para a Namecoin é Alt Chain, pois seu foco não é ser uma moeda como o Bitcoin.
  - Proposta de substituir o *Domain Name Service* (DNS) de forma descentralizada.
- IXCoin
  - Surgiu em agosto de 2011.
  - O IXCoin mantém o limite total de 21 milhões de unidades, mas aumenta a recompensa por bloco para se chegar ao limite mais rapidamente.
- Tenebrix

  - Surgiu em setembro de 2011.
  - Implementa alterações no algoritmo de *proof-of-work* do Bitcoin.
  - Algoritmo de consenso chamado de *scrypt proof-of-work*.
  - Serviu de base para o Litecoin.

- Litecoin
  - Surgiu em outubro de 2011.
  - Além de implementar o *scrypt*, reduziu o tempo de geração do bloco drasticamente em relação ao Bitcoin.
  - Alcançou boa popularidade devido às transações significativamente mais rápidas.
  - Muitas *altcoins* hoje em dia são derivadas do Litecoin.

- Bitcoin Cash
  - Surgiu em agosto de 2017.
  - Propósito de atualizar o tamanho do bloco para 8MB.
  - Alcançou boa popularidade devido às transações significativamente mais rápidas.
  - O maior *fork* em valor de mercado.

4.1.10 Visão geral

No Bitcoin, as transações são validadas por uma rede de computadores e as suas informações são armazenadas em blocos. Por isso, o nome ”cadeia de blocos” ou Blockchain. Os usuários na rede são pares entre si e são chamados de nós. Cada nó, pode executar outras funções além do protocolo P2P, essas funções são: carteira, mineração, Blockchain completa e roteamento.

As carteiras são responsáveis por armazenar e gerenciar as chaves do usuário, desta forma, elas podem ser usadas para controlar o acesso ao dinheiro do usuário, gerenciar suas chaves e endereços, acompanhar o balanço, criar e assinar as transações. Cada carteira é identificada por um endereço que deve ser informado nas transações, além disso, as transações devem ser assinadas digitalmente com a chave privada correspondente, assim é possível identificar quem tem a propriedade dos *bitcoins*, além do emissor e receptor daquela transação.

As transações são transmitidas para os demais nós da rede, através de um nó completo ou um nó leve conectado a um nó completo. Um conjunto de transações devem ser reunidas pelos mineradores formando os blocos. Em seguida, é realizado o processo de mineração, através do protocolo *proof-of-work* (PoW). Por fim, o bloco é validado e retransmitido para rede, para que seja formado um consenso.

Quando ocorre uma mudança nas regras de consenso de uma criptomoeda, a rede da mesma pode se dividir em duas cadeias. Esse tipo de bifurcação é chamado de *hard fork*. Caso as novos regras de consenso sejam adotadas e a cadeia seja continuada, essa implementação de mudanças na regra de consenso é considerada uma moeda alternativa (*altcoin*).

4.2 Ethereum

Da perspectiva da ciência da computação, o Ethereum é uma máquina de estados determinística, mas praticamente ilimitada, consistindo em um sistema de estados global e uma máquina virtual que aplica alterações a esse estado. (ANTONOPOULOS; WOOD, 2018). Entretanto, de um ponto de vista mais prático, o Ethereum é uma infraestrutura *open source* global de computação descentralizada que executa programas chamados de contratos inteligentes. Desta forma, o Ethereum usa uma Blockchain para sincronizar e armazenar as mudanças de estado do sistema, juntamente com uma criptomoeda chamada Ether para medir e restringir os custos dos recursos para execução. (ANTONOPOULOS; WOOD, 2018).

Dannen (2017) explica que redes como o Bitcoin e Ethereum são *kits* que permitem a adição de um sistema econômico em um software. Entretanto, no Ethereum, esse conceito é levado um passo adiante, com a possibilidade que os usuários têm de estabelecer contratos financeiros entre si, dentro da rede. Desta forma, o componente chave do Ethereum seria a linguagem de programação embutida, já que em relação à sua estrutura de um livro razão descentralizado, ele é semelhante ao Bitcoin.

O Ethereum possui o objetivo de criar um protocolo alternativo para construção de aplicações descentralizadas. Isso é viável graças a Blockchain com uma linguagem Turing-completa integrada, permitindo que qualquer pessoa possa escrever contratos inteligentes, aplicações descentralizadas e criar suas próprias regras arbitrárias para a propriedade, formatos de transação e funções de transição de estado. (BUTERIN et al., 2013).

Assim, o Ethereum permite que os desenvolvedores construam poderosos aplicativos com funções econômicas integradas. Enquanto fornece alta disponibilidade, auditabilidade, transparência e neutralidade, também reduz ou elimina a censura e reduz certos riscos de contraparte. (ANTONOPOULOS; WOOD, 2018).

4.2.1 Blockchain

É possível estabelecer pontos em comum e divergentes entre as *blockchains* do Bitcoin e Ethereum. A Blockchain original (Blockchain do Bitcoin), acompanha o estado das unidades de Bitcoin e seus proprietários. Dessa forma, o Bitcoin pode ser considerado como uma máquina de estados de consenso distribuído, onde transações causam uma transição do estado global, alterando o proprietário das moedas. Assim, as transições de estado são limitadas pelas regras do consenso, permitindo que haja uma eventual conversão de todos os participantes para um estado comum do sistema, após a mineração de vários blocos. (ANTONOPOULOS; WOOD, 2018).

Nesse sentido, de acordo com Dannen (2017) e Antonopoulos e Wood (2018), todas as transações do Ethereum, assim como as mudanças de estado são salvas na Blockchain, mais precisamente, nos nós da rede. Dessa forma, o Ethereum também pode ser considerado uma

máquina de estados distribuída. Mas em vez de rastrear apenas o estado da propriedade da moeda, Ethereum rastreia as transições de estado de um armazenamento de dados de uso geral, ou seja, uma estrutura que pode armazenar qualquer dado exprimível como uma tupla de chave-valor. Assim, o Ethereum possui uma estrutura que armazena tanto a chave e o valor, e usa a Blockchain para acompanhar as mudanças nesses dados ao longo do tempo. Em resumo, como um computador de uso geral, o Ethereum pode carregar código em sua máquina de estados e executar esse código, armazenando as mudanças de estado resultantes em sua Blockchain.

Portanto, duas das principais diferenças para maioria dos computadores de uso geral são que as mudanças de estado do Ethereum são regidas pelas regras do consenso e o estado é distribuído globalmente. Desso modo, o Ethereum soluciona a pergunta: "E se pudéssemos rastrear qualquer estado arbitrário e programar a máquina de estado para criar um computador distribuído operando sob consenso?". (ANTONOPOULOS; WOOD, 2018).

4.2.2 Turing completude e Ethereum

Em 1936, Alan Turing criou um modelo matemático de um computador que consiste em uma máquina de estados que manipula símbolos, lendo e os escrevendo em uma memória sequencial. Com essa construção, Turing passou a fornecer um fundamento matemático para responder (no negativo) a perguntas sobre computabilidade universal, ou seja, se todos os problemas são solucionáveis. Dessa forma, ele provou que existem classes de problemas que são incomputáveis. Alan Turing, definiu ainda que um sistema é Turing completo se ele pode ser usado para simular qualquer máquina de Turing. Tal sistema é chamado de *UTM* (Máquina de Turing universal). (ANTONOPOULOS; WOOD, 2018)

Nesse sentido, Antonopoulos e Wood (2018) define que a habilidade do Ethereum de executar um código armazenado na Blockchain enquanto lê e escreve dados na memória, faz do mesmo, um sistema Turing completo, e portanto, uma *UTM*. Dessa forma, o Ethereum pode computar qualquer algoritmo que possa ser computado por uma máquina de Turing, dadas as limitações da memória finita.

As transições de estado Ethereum são processadas pelo Ethereum Virtual Machine (EVM), uma máquina virtual baseada em pilha que executa *bytecode* (instruções em linguagem de máquina). Assim, programas EVM, são chamados de contratos inteligentes e escritos em linguagens de alto nível (por exemplo, Solidity) e compilado para bytecode para execução. (ANTONOPOULOS; WOOD, 2018).

Dannen (2017) explica que a EVM é um computador global, no qual as transações são locais e cada nó da rede executa de forma relativamente síncrona. Logo, se trata de uma máquina virtual de acesso global, composta por vários computadores menores.

Portanto, segundo Antonopoulos e Wood (2018) a principal inovação do Ethereum é combinar uma arquitetura de computação de propósito geral e computador de programas

armazenados com uma Blockchain descentralizada, deste modo criando um computador mundial com um único estado distribuído.

4.2.3 Unidades de moeda

A unidade de moeda do Ethereum é chamada de *ether*, também identificada como ETH. Em alguns lugares pode-se notar a referência ao Ethereum como moeda, porém isso é um engano, Ethreum é o sistema *ether* é a moeda. O *ether* é subdividido em unidades menores, até a menor unidade possível, chamada de *wey*. Sendo que um *ether* equivale a 1 quintilhão de *wey* (1.000.000.000.000.000.000). Dessa forma, o valor do *ether* é sempre representado internamente no Ethereum como um valor inteiro sem sinal denominado em *wei*. Quando você transaciona 1 *ether*, a transação codifica 1000000000000000000 *wei* como valor. (ANTONOPOULOS; WOOD, 2018).

4.2.4 Contas de propriedade externa e contratos

De acordo com Buterin et al. (2013), no Ethereum, o estado é composto por objetos chamados contas, com cada conta tendo um endereço de 20-bytes e as transições de estado sendo transferências diretas de valores e informações entre contas. Dessa forma, uma conta Ethereum contém quatro campos:

- O *nonce* - um contador usado para garantir que cada transação só possa ser processada uma única vez
- O saldo atual da conta em *ether*.
- O código de contrato da conta, se houver.
- O armazenamento da conta (vazio por padrão).

Conforme Dannen (2017) e Antonopoulos e Wood (2018) apresentam, os usuários da rede Ethereum podem possuir dois tipos de contas: contas privadas externas (EOA's) e contas de contrato. EOA's são contas que podem ter uma chave privada, isso significa controlar o acesso a fundos ou contratos. Já uma conta de contratos possui um código de contrato inteligente, que uma EOA simples não pode ter. Além disso, uma conta de contrato não possui uma chave privada, ela é possuída (e controlada) pelo contrato inteligente: um programa registrado na Blockchain do Ethereum e executado pelo EVM.

Os contratos, assim como os EOAs, possuem endereços e também podem enviar e receber *ethers*. No entanto, quando o destino de transação é um endereço do contrato, esse contrato é executado no EVM, usando a transação, e os dados da transação, como sua entrada. Além do *ether*, transações podem conter dados que indicam qual função específica no contrato

a ser executada e quais parâmetros passar para essa função. Dessa forma, transações podem chamar funções dentro de contratos. (ANTONOPOULOS; WOOD, 2018).

Sendo assim, como uma conta de contrato não possui uma chave privada, ela não pode iniciar uma transação. Apenas EOAs podem iniciar transações, mas os contratos podem reagir às transações chamando outros contratos, construindo uma execução complexa de caminhos. Por exemplo, um contrato pode pegar o depósito do remetente, dividi-lo em três e enviar os valores adiante a três parentes humanos diferentes. Desta forma, os contratos podem agir no lugar dos humanos para automatizar tarefas dentro de uma organização descentralizada ou mediar transações entre indivíduos que de outra forma precisariam de uma contraparte. (DANNEN, 2017; ANTONOPOULOS; WOOD, 2018).

Em resumo, Dannen (2017) explica que as EOAs possuem as seguintes características:

- Contém um balanço de *ethers*.
- São capazes de enviar transações.
- São controladas por chaves privadas.
- Não possuem códigos associados a elas.
- Possuem um banco de dados de chave/valor, onde chaves e valores são *strings* de 32 *bytes*.

Já as contas de contrato, segundo Dannen (2017) possuem as seguintes características:

- Possuem um balanço de *ethers*.
- Guardam códigos de contratos na memória.
- Podem ser acionadas por humanos, enviando uma transação ou por outros contratos através de uma mensagem.
- Quando executados, podem realizar operações complexas.
- Possuem seu próprio estado persistente e podem acionar outros contratos.
- Não possuem donos depois de serem liberados para a EVM.
- Possuem um banco de dados de chave/valor, onde chaves e valores são *strings* de 32 *bytes*.

4.2.5 Clientes

Um cliente Ethereum é uma aplicação que implementa a especificação do Ethereum e se comunica pela a rede *peer-to-peer* com outros clientes Ethereum. Sendo que, diferentes clientes interagem entre si caso eles cumpram com as especificações recomendadas e com os protocolos

padronizados para comunicação. Logo, mesmo que clientes sejam implementados por equipes diferentes e em diferentes linguagens de programação, eles seguem o mesmo protocolo e as mesmas regras, podendo assim ser usados para operar e interagir com a mesma rede Ethereum. (ANTONOPOULOS; WOOD, 2018).

De acordo com Dannen (2017), o Ethereum possui muitas aplicações clientes. Que podem funcionar como nós completos ou não. No caso do Ethereum, assim como no Bitcoin, muitas das carteiras operam como *lightweight nodes*, nós que se conectam na Blockchain para realizar funções básicas, como enviar e receber criptomoedas.

Dessa forma, como Antonopoulos e Wood (2018) explica, existe uma variedade de redes baseadas no Ethereum e grande parte delas estão em conformidade com as especificações formais definidas no Ethereum Yellow Paper, mas que podem ou não operar entre si.

Entre essas redes baseadas em Ethereum estão Ethereum, Ethereum Classic, Ella, Expanse, Ubiq, Musicoin e muitas outras. Embora sejam, de uma forma geral, compatíveis a nível de protocolo, essas redes geralmente têm recursos ou atributos que exigem que os mantenedores dos clientes Ethereum façam pequenas alterações para dar suporte a cada rede. Por isso, nem todos os clientes executam todas as *blockchains* baseadas em Ethereum. (ANTONOPOULOS; WOOD, 2018).

Segundo Antonopoulos e Wood (2018), existem seis principais clientes da rede Ethereum, escritas em seis diferentes linguagens:

- Parity, escrita em Rust
- Geth, escrita em Go
- *cpp-ethereum*, escrita em C++
- *pyethereum*, escrita em Python
- Mantis, escrita em Scala
- Harmony, escrita em Java

4.2.6 Carteiras

Segundo Antonopoulos e Wood (2018) algumas carteiras Ethereum, além de controlar o acesso ao dinheiro do usuário, gerenciar suas chaves e endereços, acompanhar o balanço, criar e assinar transações, também podem interagir com contratos. Para algumas carteiras, isso é tudo que existe. Porém, outras carteiras fazem parte de uma categoria muito mais ampla, a dos navegadores, que são interfaces para aplicativos descentralizados baseados em Ethereum, ou *DApps* (explicados com mais detalhes na seção 4.2.13). Sendo assim, não há linhas claras de distinção entre as várias categorias que são combinadas sob o termo carteira.

4.2.7 Transações e mensagens

As transações são pacotes de dados assinados originados de uma conta externa, transmitidos pela rede Ethereum, e registrados na Blockchain. Uma maneira de enxergar as transações é como uma sequência de instruções que podem desencadear uma mudança de estado ou fazer com que um contrato seja executado no EVM. Considerando que o Ethereum é uma máquina de estados global, as transações é que são responsáveis pela mudança de estado dessa máquina. Dessa forma, os contratos não executam por conta própria e o Ethereum não funciona de forma autônoma. Tudo começa com uma transação. (ANTONOPOULOS; WOOD, 2018).

Segundo Antonopoulos e Wood (2018), cada cliente e aplicativo recebe uma transação serializada a armazena na memória usando sua própria estrutura de dados interna. Assim, a serialização da rede é a única forma padrão de uma transação. Logo, uma transação é um pacote de dados binário serializado que contém o seguinte dados:

- *Nonce* - Um número de sequência, emitido pelo EOA de origem, usado para evitar a repetição da mensagem.
- *Gas price* - O preço do *gas* (em *wei*) que o originador está disposto a pagar.
- *Gas limit* - A quantidade máxima de *gas* que o originador está disposto a comprar para esta transação.
- *Recipient* - O endereço Ethereum de destino.
- *Value* - A quantidade de *ether* a ser enviada para o destino.
- *Data* - A carga de dados binários de comprimento variável.
- *v,r,s* - Os três componentes de uma assinatura digital ECDSA do EOA de origem.

No Ethereum, o *nonce* tem uma função diferente comparado com o Bitcoin, Antonopoulos e Wood (2018) apresenta que ele equivale a um valor escalar igual ao número de transações enviadas deste endereço ou, no caso de contas com código associado, o número de criações de contrato feitas por esta conta. Assim, o *nonce* é um atributo do endereço de origem; isso é, ele só tem significado no contexto do endereço de envio. No entanto, o *nonce* não é armazenado explicitamente como parte do estado de uma conta no Blockchain. Em vez disso, é calculado dinamicamente, contando o número de transações confirmadas originadas de um endereço. Portanto, o *nonce* torna cada transação única e é útil para resolver problemas como a detecção das ordens das transações e a duplicação das mesmas.

Conforme Dannen (2017) e Antonopoulos e Wood (2018) explicam, o *gas* é o combustível do Ethereum. Ele é uma unidade de medida utilizada para pagar pelas operações dentro da rede Ethereum. Ethereum usa *gas* para controlar a quantidade de recursos que uma transação

pode usar, uma vez que a mesma será processada em milhares de computadores em todo o mundo. Dessa forma, o *gas* é separado do *ether* para proteger o sistema da volatilidade que podem surgir junto com as mudanças rápidas no valor do *ether*, e também é uma maneira de gerenciar as relações importantes e sensíveis entre os custos do vários recursos pelos quais o *gas* paga (ou seja, computação, memória e armazenamento).

De acordo com Dannen (2017), o *gas* tem ainda um efeito regulatório, já que ao forçar os usuários a pagar por transações no EVM, a probabilidade de que programas intermináveis e desnecessários sejam executados é teoricamente reduzida. Dessa forma, o propósito do *gas* é duplo. Primeiro, garante uma recompensa pré-paga para os mineradores que executam código e protegem a rede, mesmo que a execução falhe por algum motivo. E em segundo lugar, ele contorna o problema da parada e garante que a execução não possa continuar mais do que o tempo pré-pago.

O *gas* é uma unidade de trabalho e não uma moeda em si, logo, não é possível mantê-lo ou acumulá-lo. O mesmo simplesmente precifica o esforço (em termos computacionais) necessário em cada etapa de uma transação. Dessa forma, para pagar pelos custos do *gas*, basta o usuário adicionar *ether* à sua conta. Não é preciso adquiri-lo separadamente; não há um *token* de *gas*. Assim, todas as operações possíveis no EVM tem um custo de *gas* associado. (DANNEN, 2017).

O campo *gasPrice* em uma transação permite que o emissor defina o preço que está disposto a pagar em troca de *gas*. Sendo o preço medido em *wei* por unidade de *gas*. Nesse sentido, as carteiras podem ajustar o *gasPrice* nas transações que originam para alcançar confirmação mais rápida das transações. Logo, quanto maior o preço do *gas*, mais rápido o transação provavelmente será confirmada. Por outro lado, transações de baixa prioridade pode ter um preço reduzido, resultando em uma confirmação mais lenta. O mínimo valor para o qual *gasPrice* pode ser definido é zero, o que significa uma taxa gratuita de transação. Desta forma, durante períodos de baixa demanda por espaço em um bloco, tais transações podem muito bem ser mineradas. (ANTONOPOULOS; WOOD, 2018).

Outro campo importante relacionado ao *gas* é o *gasLimit*. Em termos simples, ele dá o número máximo de unidades de *gas* que o originador da transação está disposto a comprar para completar a transação. Para simples pagamentos, ou seja, transações que transferem *ether* de um EOA para outro EOA, a quantidade de *gas* necessária é fixada em 21.000 unidades. Assim, para calcular quanto *ether* uma transação custa, basta multiplicar 21.000 pelo *gasPrice*. (ANTONOPOULOS; WOOD, 2018).

Porém, se o endereço de destino de uma transação for um contrato, o valor de *gas* necessário pode ser estimado, mas não pode ser determinado com precisão. Isso porque um contrato pode avaliar diferentes condições que levam a diferentes caminhos de execução, com diferentes custos totais de *gas*. O contrato pode executar apenas um cálculo simples ou um mais complexo, dependendo de condições que não podem ser previstas. Deste modo, quando uma

transação é transmitida, uma das primeiras etapas de validação é a verificação se a conta de onde se originou tem *ether* suficiente para pagar o *gasPrice*. Porém, o valor não é realmente deduzido da conta até que a transação termine de ser executada. Logo, o emissor só é cobrado pelo *gas* consumido na transação, mas ele precisa ter saldo suficiente para o valor máximo que ele está disposto a pagar antes de enviá-la. (ANTONOPOULOS; WOOD, 2018).

Antonopoulos e Wood (2018) explica que, o destinatário é especificado no campo *recipient*. Esse campo possui 20 bytes correspondentes ao endereço, onde o mesmo pode estar relacionado à uma EOA ou um contrato.

A carga útil principal de uma transação está contida em dois campos: *value* (valor) e *data* (dados). Assim, as transações podem ter valor e dados, apenas valor, apenas dados ou nem valor nem dados. Todas as quatro combinações são válidas: uma transação com apenas valor é um pagamento, uma transação com apenas dados é uma invocação, uma transação com valor e dados é tanto um pagamento quanto um uma invocação e uma transação sem valor nem dados é improvável, pois representa um desperdício de *gas*, mas é possível. (ANTONOPOULOS; WOOD, 2018).

De acordo com Antonopoulos e Wood (2018) uma transação não possui um campo contendo especificamente o endereço de destino já que é possível calculá-lo a partir da assinatura ECDSA. Desta forma os campos referentes a assinatura digital, como visto na seção 3.1.2, são úteis para atestar a integridade, autenticidade e o endereço de origem da transação.

De acordo com Buterin et al. (2013), os contratos também podem enviar mensagens para outros contratos. As mensagens são objetos virtuais que nunca são serializados e existem apenas no ambiente de execução Ethereum. Dessa forma, uma mensagem contém:

- O remetente da mensagem (implícito).
- O destinatário da mensagem
- A quantidade de *ether* a ser transferida junto com a mensagem.
- Um campo de dados opcional.
- Um valor *Gas price*.

Uma mensagem na rede Ethereum funciona de forma como uma transação interna, no entanto, ela é produzida por um contrato e não por um agente externo. Além do fato de nunca serem serializadas, as mensagens são enviadas apenas dentro da EVM. Assim como uma transação, uma mensagem leva à execução do código de conta do destinatário. Dessa maneira, os contratos podem interagir com outros contratos exatamente da mesma forma que os agentes externos. (BUTERIN et al., 2013).

4.2.8 Blocos

As transações e mudanças de estado na rede Ethereum são segmentadas em blocos. Cada bloco é verificado e validado antes que o próximo bloco seja colocado acima dele. Dessa forma, os nós da rede não precisam avaliar a confiabilidade de cada bloco no histórico da rede, eles apenas verificam se o bloco pai é o bloco canônico mais recente. Isso é verificado apenas checando se o novo bloco contêm o *hash* correto das suas transações pai e estados. Após isso, eles simplesmente computam o balanço presente nas contas. (DANNEN, 2017).

Conforme explicado por Dannen (2017), no Ethereum, o intervalo entre a criação de blocos é mantido com o menor valor possível, para manter a confirmação rápida das transações. Em média, o tempo dos blocos é cerca de 15 segundos a partir da escrita.

4.2.9 Contratos inteligentes e Solidity

Conforme explicado na seção 4.2.4, existem dois tipos de contas no Ethereum: contas proprietárias externas (EOAs) e contas de contratos. As EOAs são controladas pelos usuários, muitas vezes, por meio de software como um aplicativo de carteira que é externo à plataforma Ethereum. Em contraste, contas de contrato são controlada por códigos de programa, os chamados contratos inteligentes (*smart contracts*) que são executados pela Máquina Virtual Ethereum (EVM). Sendo assim, resumidamente, EOAs são contas simples sem nenhum código associado ou armazenamento de dados, enquanto as contas de contrato têm código associado e armazenamento de dados. (ANTONOPOULOS; WOOD, 2018).

Desta forma, EOAs são controlados por transações criadas e assinadas criptograficamente com uma chave privada no mundo real externo e independente do protocolo. Enquanto as contas de contrato não possuem chaves privadas e, portanto, se controlam da maneira predeterminada prescrita por seus código do contrato. Sendo, ambos os tipos de contas identificadas por um endereço Ethereum. (ANTONOPOULOS; WOOD, 2018).

Segundo Dannen (2017), os contratos inteligentes são como classes na programação orientada a objetos. Logo, escrever contratos inteligentes é simplesmente o ato de escrever código em linguagem de programação para ser executado na rede Ethereum. Assim, quando o código é executado, unidades de valor podem ser transferidas de forma simples como dados.

Para Antonopoulos e Wood (2018), o termo contrato inteligente é usado para se referir a programas de computador imutáveis que são executados de forma determinística no contexto de uma EVM como parte do protocolo da rede Ethereum. Portanto, contratos inteligentes são simplesmente, programas de computador e não possuem nenhum significado legal nesse contexto. Eles são considerados imutáveis, já que uma vez implantado, o código de um contrato inteligente não pode ser alterado, sendo a única maneira de modificar um contrato inteligente é implantando uma nova instância.

Logo, contratos no Ethereum não devem ser vistos como algo que deve ser realizado ou

cumprido. Eles são como como agentes autônomos dentro do ambiente de execução do Ethereum, sempre executando uma parte específica do código quando solicitado por uma mensagem ou transação, e tendo controle direto sobre seu próprio saldo de *ethers* e seus próprios dados armazenados. (BUTERIN et al., 2013).

De acordo com Antonopoulos e Wood (2018) os contratos inteligentes são determinísticos, uma vez que resultado de sua execução é o mesmo para todos que o executam, dado o contexto da transação que iniciou sua execução e o estado da Blockchain Ethereum naquele momento. Outra característica dos contratos inteligentes é que eles operam com um contexto de execução muito limitado. Já que só podem acessar seu próprio estado, o contexto da transação que os chamou, e algumas informações sobre os blocos mais recentes.

Assim, eles contribuem para formação de um computador mundial descentralizado. Uma vez que a EVM é executado como uma instância local em cada nó Ethereum, mas todas as instâncias operam no mesmo estado inicial e produzem o mesmo estado final. (ANTONOPOULOS; WOOD, 2018).

Dannen (2017) e Antonopoulos e Wood (2018) explicam, que a linguagem Solidity é muito usada para criação dos contratos inteligentes, porém eles podem ser escritos em outras linguagens, como Vyper por exemplo. A linguagem Solidity foi criada por Dr. Gavin Wood, como um linguagem para escrever contratos inteligentes com recursos para apoiar a execução no ambiente descentralizado do Ethereum. A linguagem Solidity é bastante intuitiva para programadores que já estão familiarizados com outras linguagens, como Javascript, Java e C.

Por possuir atributos que são comuns a outras *blockchains*, a linguagem Solidity acabou sendo usada para codificar contratos inteligentes em várias outras plataformas. Assim, a principal iniciativa do projeto Solidity é o compilador *solc*, que converte programas escritos em Solidity para EVM bytecode. (ANTONOPOULOS; WOOD, 2018).

4.2.10 Tokens

Para Antonopoulos e Wood (2018), *tokens* são abstrações baseadas em Blockchain que podem ser possuídas e que representam ativos, moeda ou direitos de acesso. Segundo Dannen (2017) os *tokens* como todas as formas de dinheiro também podem ser vistos como contratos sociais ou acordos entre grupos de usuários. Em outras palavras, o fato dos membros de uma comunidade concordarem que um *token* equivale a dinheiro, se trata de um acordo implícito entre eles.

Como explicado por Antonopoulos e Wood (2018), os *tokens* podem possuir muitas funções diferentes, em alguns casos, de forma simultânea. Alguns exemplos de usos são:

- Moeda - Um *token* pode servir como uma forma de moeda, com um valor determinado através do comércio privado.

- Recurso - Um *token* pode representar um recurso ganho ou produzido em uma economia de compartilhamento ou ambiente de compartilhamento de recursos; por exemplo, um *token* de armazenamento ou de CPU representando recursos que podem ser compartilhados em uma rede.

- Ativo - Um *token* pode representar uma propriedade intrínseca ou extrínseca, tangível ou intangível; por exemplo, ouro, imóveis, um carro, petróleo, energia, itens em um jogo, etc.

- Acesso - Um *token* pode representar direitos de acesso a uma propriedade física ou virtual, como um fórum de discussão, um site exclusivo, um quarto de hotel ou um carro alugado.

- Patrimônio - Um *token* pode representar o patrimônio dos acionistas em uma organização digital ou entidade legal.

- Voto - Um *token* pode representar direitos de voto em um sistema digital ou legal.

- Colecionável - Um *token* pode representar um colecionável digital ou colecionável físico (uma pintura, por exemplo).

- Identidade - Um *token* pode representar uma identidade digital (por exemplo, avatar) ou identidade legal (por exemplo, ID nacional).

- Atestado - Um *token* pode representar uma certificação ou atestado de fato por alguma autoridade ou por um sistema de reputação descentralizado (por exemplo, registro de casamento, certidão de nascimento, diploma universitário).

- Utilitário - Um *token* pode ser usado para acessar ou pagar por um serviço.

Sendo assim, os *tokens* podem ser fungíveis quando podemos substituir qualquer unidade do *token* por outra sem qualquer diferença em seu valor ou função ou podem ser não-fungíveis, quando representam um item único e, portanto, não são intercambiáveis. Por exemplo, um *token* que representa a propriedade de uma pintura específica de Van Gogh não é equivalente a outro *token* que representa um Picasso, mesmo que eles possam fazer parte do mesmo sistema de *token* de propriedade de arte. Dessa forma, cada *token* não-fungível é associado a um identificador exclusivo, como um número de série. (ANTONOPOULOS; WOOD, 2018).

4.2.11 Mineração

De acordo com Dannen (2017) o processo de mineração no Ethereum funciona da seguinte forma: sempre que um bloco é criado, ele é baixado, processado e validado pelos nós da rede. Durante esse processo, cada nó executa todas as transações contidas no bloco. Além disso, para cada transação em um bloco, o *EVM* realiza os seguintes passos:

1. Verifica se a transação está no formato correto. Se tem o número certo de valores. Se a assinatura é válida. Se o *nonce* na transação corresponde ao *nonce* da conta. Caso alguma coisa esteja faltando, um erro é devolvido ao emissor da transação.

2. Calcula a taxa de transação, multiplicando o valor de trabalho necessário pelo preço do *gas*. Em seguida, deduz a taxa do saldo da conta do usuário e incrementa o *nonce* do remetente (contador de transações). Se não houver éter suficiente na conta, retorna um erro.

3. Inicializa o pagamento do *gas*; deste ponto em diante, uma certa quantidade de *gas* é retirada por byte processado na transação.

4. Se a conta de recebimento ainda não existir, ela será criada. Se o endereço de recebimento for um endereço de contrato, o código do contrato é executado. Isso continua até que o código termine a execução ou o pagamento do *gas* se esgote.

5. Se a conta de envio não possuir *ether* suficiente para concluir a transação, ou o *gas* acabar, todas as mudanças a partir desta transação são revertidas. Uma ressalva são as taxas, que ainda vão ao minerador e não são reembolsadas.

6. Se a transação gerar um erro por qualquer outro motivo, o *gas* é reembolsado para o remetente , assim como, quaisquer taxas associadas ao *gas*, usadas pelo minerador.

Todo esse processo ocorre no protocolo *proof-of-work*, porém no dia 15 de setembro de 2022 o Ethereum lançou uma atualização chamada "*The merge*" que muda o protocolo de validação de transações de *proof-of-work* (PoW) para *proof-of-stake* (PoS).

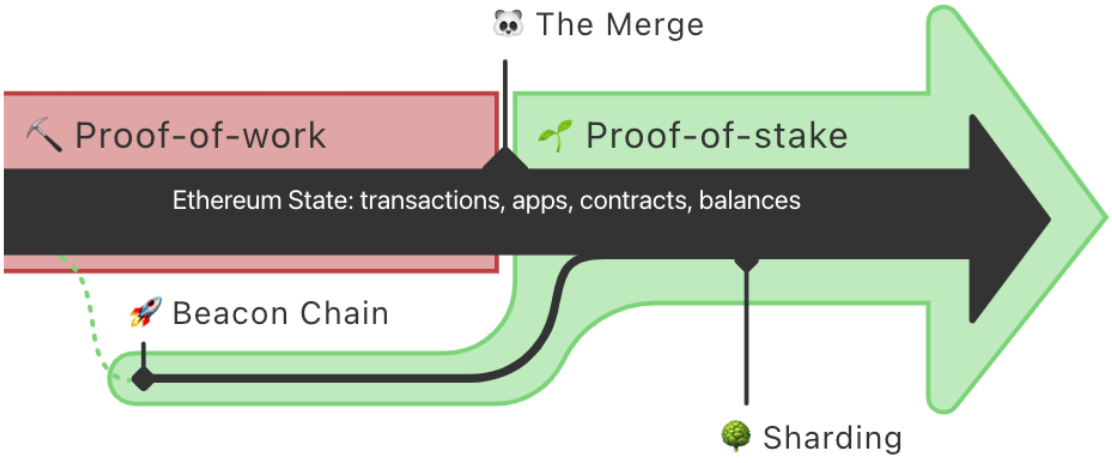

Figura 14 – Ethereum: *The Merge* (NAIJA, 2022)

A Figura 14 apresenta a mudança do protocolo *proof-of-work* (em vermelho) para *proof-of-stake* (em verde) com a atualização *The Merge* no Ethereum. A Figura mostra também a Beacon Chain, que é o nome da Blockchain *proof-of-stake* original do Ethereum, que foi criada para para garantir que a lógica de consenso de prova de participação era sólida e sustentável antes de implementá-la na rede principal do Ethereum. Assim, a Beacon Chain foi integrada à cadeia de prova de trabalho da Ethereum original em setembro de 2022 através da atualização The Merge. (ETHEREUM.ORG, 2023).

4.2.12 *Proof of Stake*

Conforme Saleh (2021) explica, o protocolo de validação *proof-of-work* (PoW) exige que os mineradores, responsáveis pela validação dos blocos na rede participem de uma competição entre si. Essa competição se dá em busca da resolução de um problema, o que gera um enorme gasto de poder de processamento e consequentemente, energia. Logo, em busca de solucionar esse problema a comunidade Blockchain cogitou diversas alternativas ao protocolo PoW. Nesse sentido, uma das alternativas é o protocolo *proof-of-stake* (PoS).

Em geral, o protocolo *proof-of-stake* ou prova de participação, funciona da seguinte forma. A Blockchain é composta por um conjunto de validadores, e qualquer um que detenha a criptomoeda base, no caso *ether* pode se tornar um validador ao enviar um tipo especial de transação que bloqueia seu *ether* em um depósito. Os validadores então, se revezam propondo novos blocos e votando no próximo bloco válido, e o peso do voto de cada validador depende do tamanho de seu depósito (ou seja, *stake*). (ANTONOPOULOS; WOOD, 2018).

Pujari et al. (2022) explicam que para participar como validador, um usuário deve depositar 32 ETH no contrato de depósito e executar três softwares separados: um cliente de execução, um cliente de consenso e um validador. Ao depositar sua ETH, o usuário ingressa em uma fila de ativação que limita a taxa de novos validadores ingressando na rede. Uma vez ativados, os validadores recebem novos blocos de *peers* na rede Ethereum. As transações entregues no bloco são executadas novamente e a assinatura do bloco é verificada para garantir que o bloco seja válido. O validador então envia um voto (chamado de atestado) a favor daquele bloco pela rede.

Enquanto na prova de trabalho, o tempo dos blocos é determinado pela dificuldade de mineração, na prova de participação, o tempo é fixo. O tempo na prova de participação Ethereum é dividido em *slots* (12 segundos) e épocas (32 *slots*). Um validador é selecionado aleatoriamente para ser um proponente de bloco em cada *slot*. Este validador é responsável por criar um novo bloco e enviá-lo para outros nós da rede. Também em cada *slot* é escolhido aleatoriamente um comitê de validadores, cujos votos são utilizados para determinar a validade do bloco proposto. (PUJARI et al., 2022).

É importante ressaltar que um validador corre o risco de perder seu depósito se o bloco

em que ele apostou é rejeitado pela maioria dos validadores. Por outro lado, os validadores ganham uma pequena recompensa, proporcional à sua aposta depositada, por cada bloco que é aceito pela maioria. Assim, PoS força os validadores a agir honestamente e seguir as regras de consenso, por um sistema de recompensa e punição. A principal diferença entre PoS e PoW é que a punição em PoS é intrínseca a Blockchain (por exemplo, perda de *ether* apostado), enquanto em PoW a punição é extrínseca (por exemplo, perda de fundos gastos com eletricidade). (ANTONOPOULOS; WOOD, 2018).

4.2.13 DApps

Desde os primeiros dias do Ethereum, a visão dos fundadores era muito mais ampla do que contratos inteligentes: nada menos do que reinventar a *web* e criar um novo mundo de DApps (aplicações descentralizadas), apropriadamente chamado de *web3*. Os contratos inteligentes são uma forma de descentralizar a lógica de controle e as funções de pagamento dos aplicativos. Em resumo, os DApps Web3 tratam da descentralização de todos os outros aspectos de um aplicativo: armazenamento, mensagens, nomes, etc. (ANTONOPOULOS; WOOD, 2018).

De acordo com Antonopoulos e Wood (2018), um DApp é uma aplicação que é totalmente, ou de forma majoritária, descentralizada. Isso, considerando todos os possíveis aspectos de uma aplicação que podem ser descentralizados:

- Backend
- Frontend
- Armazenamento de dados
- Comunicação e mensagens
- Resolução de nomes

Na Figura 15 é possível observar um vislumbre do que seria a Web3, com vários serviços rodando em uma rede descentralizada.

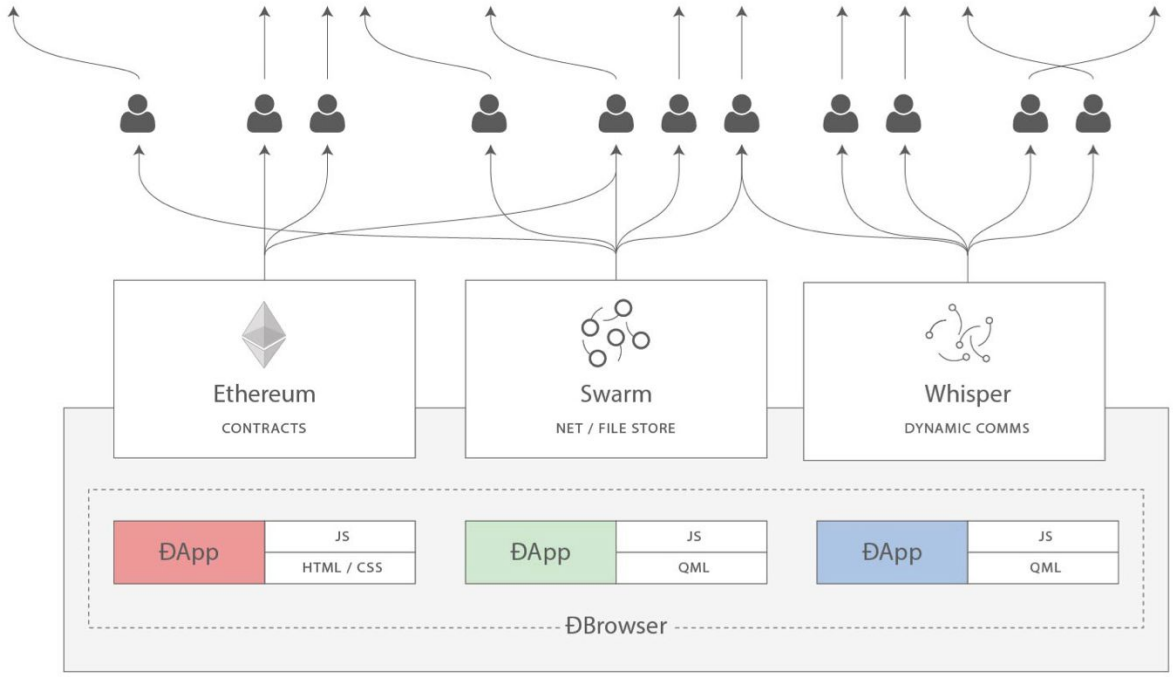

Figura 15 – *Web3*: Uma web descentralizada usando contratos inteligentes e tecnologias P2P (ANTONOPOULOS; WOOD, 2018)

Nesse sentido, Antonopoulos e Wood (2018) apresentam que há muitas vantagens em criar um DApp que uma arquitetura típica não pode fornecer:

- **Disponibilidade** - Como a lógica de negócios é controlada por um contrato inteligente, um *backend* descentralizado seria totalmente distribuído e gerenciado por uma plataforma Blockchain. Ao contrário de uma aplicação implantada em um servidor centralizado, um DApp não possui tempo de inatividade e continua disponível enquanto a plataforma está operando.

- **Transparência** - A natureza de armazenamento dos dados na cadeia de um DApp permite que todos inspecionem o código e tenham mais certeza sobre sua função. Qualquer interação com o DApp será armazenada para sempre na Blockchain.

- **Resistência à censura** - Contanto que um usuário tenha acesso a um nó Ethereum (executando um se necessário), o usuário sempre poderá interagir com um DApp sem interferência de qualquer controle centralizado. Nenhum prestador de serviço, ou mesmo o proprietário do contrato inteligente, pode alterar o código a partir do momento em que este for implantado na rede.

4.2.14 Moedas alternativas ao Ethereum

De acordo com Antonopoulos e Wood (2018), Cavalcanti (2022) e IQ (2018), algumas das principais *altcoins* do Ethereum são:

- Ethereum Classic
  - *Fork* aconteceu em julho de 2016.
  - O *fork* ocorreu após o aplicativo construído através do DAO (um contrato inteligente) ser hackeado, causando um prejuízo de cerca de 5% de todos os ETH que circulavam até aquele momento (mais precisamente 3.6 milhões de ETH).
  - Houve a proposta de reverter a rede para o passado, alterando o histórico dos blocos e desfazendo o *hack*.
  - Um número de pessoas no ecossistema discordou dessa mudança, acreditando imutabilidade deve ser um princípio fundamental da Blockchain Ethereum. Assim, eles optaram por continuar a cadeia original sob o apelido de Ethereum Classic (ETC).
- EtherZero
  - Possui um conjunto de mudanças em relação ao Ethereum.
  - Criada em janeiro de 2018.
  - Reduziu o intervalo entre blocos, de 15 para 10 segundos
  - Pagamento instantâneo.
  - Maior escalabilidade.

4.2.15 Visão geral

Em resumo, o Ethereum é uma infraestrutura de computação descentralizada que executa programas chamados de contratos inteligentes. Ele se utiliza de uma Blockchain para sincronizar e armazenar as mudanças no sistema, e de uma criptomoeda chamada *ether* para realizar transações e pagamentos relativos aos contratos. Dessa forma, os componentes mais importantes do Ethereum são a sua Blockchain e a máquina virtual (EVM) Turing-completa presente em cada nó, que permite que qualquer pessoa possa escrever contratos inteligentes, aplicações descentralizadas (DApps) e criar suas próprias regras contratuais, formatos de transação e funções de transição de estado.

No Ethereum, o estado é composto por objetos chamados contas. Sendo que os usuários da rede podem possuir dois tipos de contas: contas privadas externas (EOA's) e contas de contrato. Os usuários interagem com a rede através de aplicações clientes que implementam a especificação do Ethereum e se comunicam pela a rede *peer-to-peer* com outros clientes.

As carteiras são um tipo de cliente que permite: controlar o acesso ao dinheiro do usuário, gerenciar suas chaves e endereços, acompanhar o balanço, criar e assinar transações e também podem interagir com os contratos. As transações são pacotes de dados assinados originados de uma conta externa, transmitidos pela rede Ethereum, e registrados na Blockchain.

Os contratos são como uma sequência de instruções que podem desencadear uma mudança de estado ou executar outros contratos. Eles executam na EVM.

Os *tokens* são abstrações baseadas em Blockchain que podem ser possuídas e que representam ativos, moeda ou direitos de acesso.

O processo de mineração no Ethereum tem como base o protocolo de validação *proof-of-stake* (PoS). Onde os validadores, se revezam propondo novos blocos e votando no próximo bloco válido, e o peso do voto de cada validador depende do tamanho de seu depósito (ou seja, *stake*).

5 Aspectos econômicos

5.1 Criptomoedas e moedas Fiat

Conforme explicado por Soares (2021), moedas são uma forma de trocar bens e serviços, já que elas surgiram da necessidade de se quantificar e atribuir valor as coisas. Dessa forma, as moedas chamadas Fiat (ou fiduciárias) são as moedas adotadas em países, regiões ou continentes; como o Euro, Real e o Dólar por exemplo. As moedas Fiat, possuem uma estrutura determinada pelas políticas monetárias de seus países. As criptomoedas, possuem uma estrutura e política definidas por um conjunto de regras fixas, controladas por algoritmos distribuídos em todo o mundo. Em outras palavras, as criptomoedas, ao contrário das moedas Fiat, geralmente, não estão sujeitas a regulação e controle de governos e outras entidades como o Banco Central. (BARBOSA, 2016; SICHEL; CALIXTO, 2018).

5.2 Utilização das criptomoedas

De acordo com Baptista (2019) na fase inicial do Bitcoin, os usuários mais notáveis estavam relacionados à atividades ilícitas como a compra de bens ilegais. Nesse sentido, inicialmente o Bitcoin possuía 2 principais perfis de usuários:

- Entusiastas da área de tecnologia.
- Usuários com fins ilícitos.

Essa privacidade se deve as tecnologias empregadas e a natureza do ativo, que permite que se faça pagamentos de forma anônima e sem entidades externas controlando as transações. Entretanto, com o passar do tempo, o número de usuários acabou crescendo e os perfis de uma forma geral acabaram mudando. (BAPTISTA, 2019).

A Figura 16 apresenta o crescimento de número de usuários da internet e das criptomoedas ao longo do tempo:

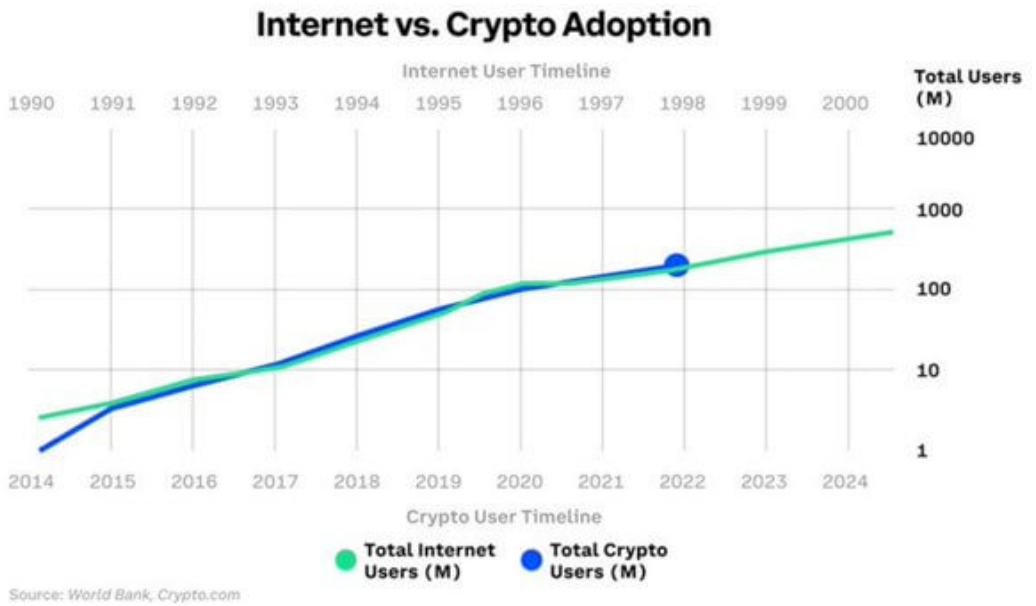

Figura 16 – Internet vs Crypto Adoption (WAN, 2021)

Wan (2021) explica que há uma correlação entre o crescimento em número de usuários da internet e das criptomoedas e que a Web3.0 pode tornar a internet e a Blockchain ainda mais integradas, o que aumentaria exponencialmente a adoção das criptomoedas.

5.3 Investimentos em criptomoedas

De acordo com Figueiredo (2020), as primeiras transações em Bitcoin se deram, principalmente, entre os próprios desenvolvedores e mineradores, nesse período inicial, a moeda não tinha quase nenhum valor, já que, o seu preço é determinado pela oferta e demanda do mercado.

Segundo Figueiredo (2020) e CoinMarketCap (2022), um dos primeiros que registros que se têm do valor do Bitcoin é de US$0,00076. Em contraste, no ano de 2021 o valor do Bitcoin chegou a US$60.000,00. A Figura 17 apresenta o gráfico do valor do Bitcoin de 2013 a 2022:

Figura 17 – Valor do Bitcoin (COINMARKETCAP, 2022)

De acordo com Rauchs, Hileman et al. (2017), a capitalização do mercado de criptomoedas cresceu mais de três vezes desde 2016. Muito desse crescimento se deve não só ao Bitcoin, mas também ao Ethereum e várias criptomoedas disponíveis no mercado como mostram as Figuras 18 e 19:

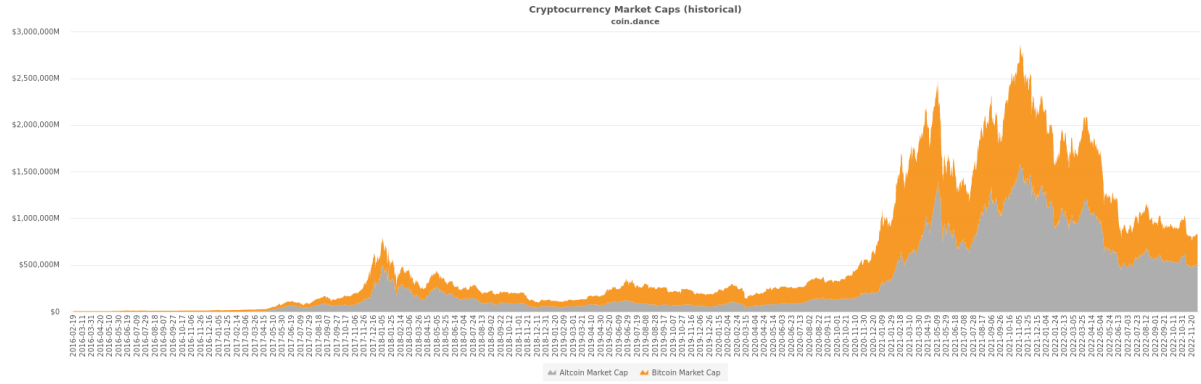

Figura 18 – Capitalização do mercado de criptomoedas (COINDANCE, 2022)

A Figura 18 apresenta um gráfico com a capitalização do Bitcoin representada na cor laranja e das *altcoins* representadas na cor cinza.

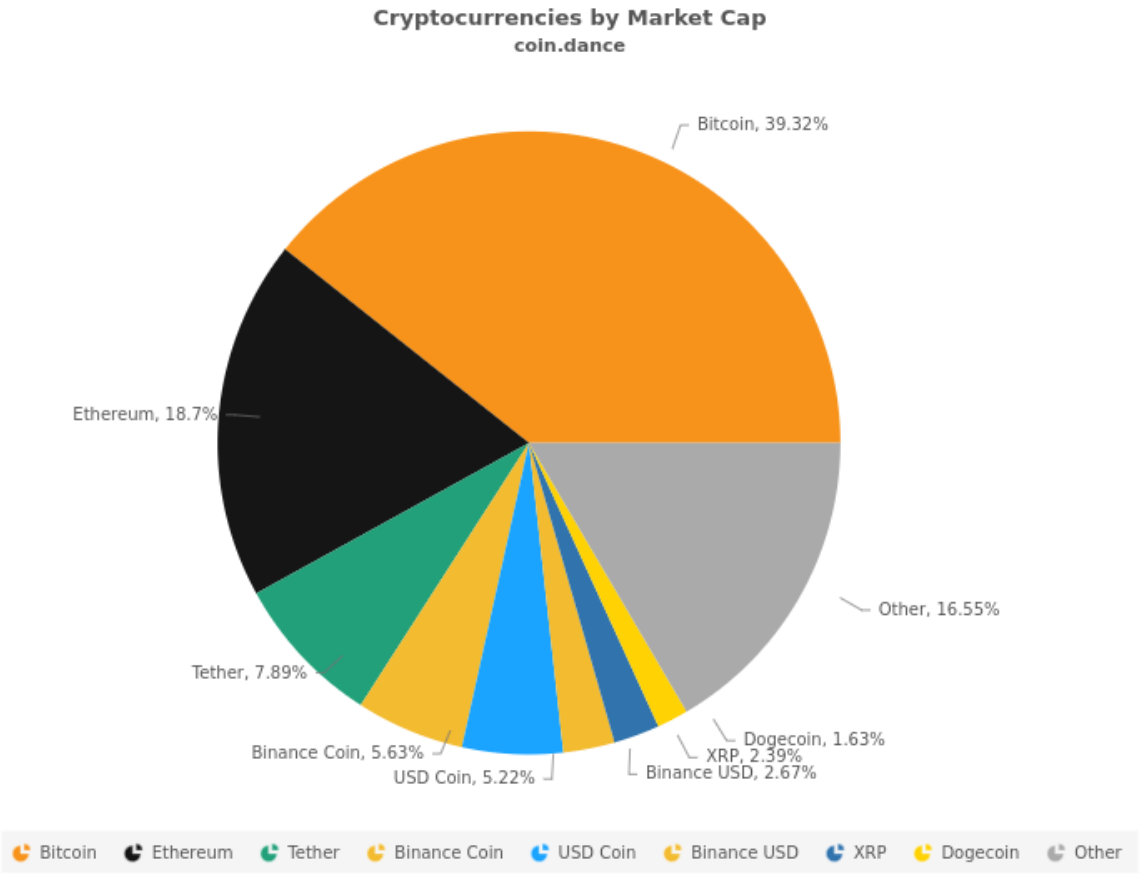

Figura 19 – Capitalização por criptomoedas (COINDANCE, 2022)

A Figura 19 apresenta um gráfico porcentagem de capitalização de cada moeda em relação ao do mercado de criptomoedas.

Após um certo tempo de funcionamento da rede, começaram a surgir serviços que aceitavam pagamento em Bitcoin, atraídas em razão da agilidade e privacidade do sistema. Da mesma forma, surgiram também casas de câmbio e corretoras especializadas em moeda digital. Sendo que atualmente, mais de 400 corretoras operam com o Bitcoin no mundo e empresas como Microsoft e Dell, o aceitam como forma de pagamento. (FIGUEIREDO, 2020; BAPTISTA, 2019).

No entanto, Figueiredo (2020) explica que muitas corretoras tradicionais sofrem com ataques e perdas financeiras, além de restrições regulatórias e governamentais. Assim, problemas com essas corretoras fomentam a procura por corretoras descentralizadas.

5.3.1 Mercado e valor

Conforme Brochado (2018) apresenta, há uma relação entre a atratividade da moeda para o investidor e seu preço. Nesse sentido, o Bitcoin atua muitas vezes como um ativo, devido a sua volatilidade e natureza especulativa. Dessa forma, quando se compara o valor do Bitcoin com outros ativos, é possível perceber que ele se comporta de forma semelhante ao dólar americano e ao ouro, entretanto o Bitcoin apresentam uma volatilidade superior. Através das Figuras 17, 20 e 21 é possível observar a volatilidade do Bitcoin, Dólar e Ouro, respectivamente.

Figura 20 – Índice do Dólar de 2013 a 2022 (TRADINGECONOMICS, 2022)

Figura 21 – Valor do Ouro de 2013 a 2022 (TRADINGECONOMICS, 2022)

Assim, segundo Brochado (2018), existem diversos fatores que podem explicar o preço e comportamento do Bitcoin, como:

- Fatores tecnológicos como a dificuldade de mineração e *hash rate*, além do reconhecimento público nas redes sociais.
- Fatores econômicos no geral como a inflação e taxa de juros.
- Fatores econômicos do Bitcoin como a oferta da moeda, transações, valor e volume de *bitcoins*.
- Atividade de mercado como volume transacionado e volatilidade, além de custos de transação em mercado secundário.
- Preço de outros ativos e criptomoedas.

5.4 Ecossistema financeiro

De acordo com Rauchs, Hileman et al. (2017) e Brochado (2018), existem vários agentes econômicos que oferecem serviços relacionados as criptomoedas e que aproveitam de alguma forma das vantagens desse sistema financeiro. Assim, o ecossistema financeiro das criptomoedas é composto de diversos atores, que constroem interfaces entre as *blockchains*, as finanças tradicionais e vários setores econômicos. Esses atores podem ser classificados em quatro principais categorias, que são:

- *Exchanges* (corretoras descentralizadas) que atuam na compra, venda e troca de criptomoedas (por outras criptomoedas ou moedas 'fiat' nacionais).
- *Wallets* (carteiras) que atuam na armazenamento de criptomoedas de forma segura através do gerenciamento de chaves (*handling key management*).
- *Payments* (pagamentos), serviços que atuam na facilitação dos pagamentos usando criptomoedas.
- *Mining* (mineração), serviços que visam assegurar o funcionamento do *ledger* global (Blockchain).

5.4.1 Corretoras descentralizadas

Brochado (2018) relata que as corretoras são serviços online relacionados a compra e venda de criptomoedas e outros ativos digitais. Assim, as corretoras são componentes importantes no ecossistema, já que as mesmas possibilitam a ligação das criptomoedas com a economia real, em que as transações são dadas em moedas locais.

Conforme apresentado por Figueiredo (2020), as corretoras descentralizadas, também chamadas de DEX possibilitam ao investidor ter controle sobre os seus próprios fundos. Diferente das corretoras tradicionais, elas funcionam através de contratos inteligentes e não armazenam dados das carteiras e transações em um servidor central.

Assim, o processo de uma transação consiste nos usuários depositarem em um contrato inteligente a quantidade a ser trocada e uma vez que as transferências são realizadas, cada parte recebe o devido valor em sua carteira. Portanto, esse processo evita a intervenção de autoridades e minimiza a ação de hackers, suprimindo o ponto de falha das soluções centralizadas. (FIGUEIREDO, 2020).

Alguns exemplos de *exchanges* são Bitfinex, Bitflyer e kraken.

5.4.2 Carteiras

Conforme explicado por Brochado (2018), carteiras são aplicações usadas para enviar e receber criptomoedas através do gerenciamento de chaves públicas e privadas criptográficas por um prestador de serviços. Muitas carteiras são *open sources*, ou seja possuem o seu código aberto e disponível na internet. Além disso, muitas carteiras oferecem diferentes formatos, possibilitando a interação dos usuários através de diferentes plataformas, como *mobile* e *desktop*.

Outro ponto interessante das carteiras é que elas podem oferecer outros serviços além do gerenciamento das chaves e transações, como a troca de moedas integrada, ligação aos cartões de crédito e débito, seguro, envio por email e sms, etc. (BROCHADO, 2018).

Alguns exemplos de carteiras são MetaMask, Trust Wallet e Keplr Wallet.

5.4.3 Serviços de pagamento

De acordo com Brochado (2018) e Rauchs, Hileman et al. (2017) os sistemas de criptomoeda possuem redes de processamento de transações denominadas *native token*, apesar disso, muitos usuários preferem usar serviços de pagamentos e transferências oferecidos por terceiros. Dessa forma, as empresas de pagamento funcionam como interfaces entre as demais empresas, o sistema financeiro tradicional e o ecossistema das criptomoedas. Nesse sentido, o setor de pagamentos pode ser dividido em quatro categorias:

- Serviços de transferência de dinheiro - serviços de pagamento que funcionam de forma internacional possibilitando a transferência de modas nacionais para indivíduos. Além disso podem incluir serviços de transferência de remessas e serviços de pagamento de contas.
- Pagamentos B2B - serviços que proveem pagamento para empresas, dados em moedas nacionais e podem ou não ocorrer através de fronteiras.
- Serviços de comércio - serviços que processam pagamentos para mercados em processo de aceitação das criptomoedas. Podem fornecer serviços comerciais adicionais, como integrações de carrinho de compras e terminais de pontos de venda
- Plataformas de propósito geral - plataformas que proveem uma variedade de serviços de transferência de criptomoedas incluindo pagamentos instantâneos para outros usuários na mesma plataforma usando criptomoedas e/ou moedas nacionais, folha de pagamento, entre outros serviços.

Alguns exemplos de empresas que atuam com serviços de pagamento são CoinGate, Coinbase e Abra.

5.4.4 Mineração

Para Brochado (2018), os mineradores são fundamentais no ecossistema das criptomoedas, já que os mesmos são responsáveis por agrupar as transações em novos blocos e adicioná-las a Blockchain. Assim, os mineradores oferecem recursos computacionais para garantir a validade da Blockchain em troca de novas moedas e taxas de transação.

Contudo, de acordo com Brochado (2018) a atividade de mineração evoluiu de um simples *hobby* praticado pelos primeiros adeptos com computadores pessoais, para uma grande indústria que utiliza *hardware* especializado para prática. Dessa forma, podem ser nomeados cinco tipos de atores envolvidos na atividade de mineração:

- Produtores de *hardware* para mineração - empresas dedicadas a produzir e comercializar *hardware* especializado para mineração.

- *Pools* de mineração - reúnem os recursos computacionais de diversos mineradores (pessoas ou empresas) para aumentar a chance de mineração de novos blocos e por consequência, as chances de receber uma recompensa. As recompensas são divididas entre os participantes com base na quantidade de recurso computacional oferecido por cada um.
- Mineradores - a atividade de mineração pode ser feita por pessoas (de forma individual) ou empresas.
- Serviços de mineração na nuvem - possibilitam que os indivíduos participem do processo de mineração sem a necessidade de executar um *hardware* próprio.
- Serviços de alojamento remoto - oferecem o serviço de armazenamento e manutenção do equipamento de mineração de indivíduos.

Alguns exemplos de plataformas, empresas e produtos relacionados a mineração são Antpool, Bitmain e StormGain.

6 Análise comparativa: Bitcoin e Ethereum

O Bitcoin e Ethereum compartilham de muitos elementos em comum como: uma rede *peer-to-peer* que conecta os participantes, um algoritmo de consenso, o uso de primitivas criptográficas como assinaturas digitais e *hashes* e uma moeda digital. Por outro lado, elas se diferem em alguns aspectos que vão desde o propósito a construção das criptomoedas em si.

Dessa forma, esta seção visa apresentar uma breve análise comparativa entre o Bitcoin e o Ethereum em diferentes quesitos. O objetivo não é definir qual das criptomoedas é a melhor, e sim, apresentar as principais diferenças entre elas, baseado nas informações apresentadas nesse trabalho.

6.1 Histórico

O Bitcoin foi criado com o propósito de solucionar alguns problemas existentes no sistema financeiro tradicional, problemas esses que foram agravados com a crise econômica de 2008. Nesse sentido, o Bitcoin foi lançado com a proposta de ser um sistema ponto a ponto de dinheiro eletrônico. Ele criou a nova tecnologia do Blockchain e incentivou o surgimento de novas criptomoedas, dentre elas, o Ethereum. Que surgiu em 2013, com o propósito de criar contratos inteligentes que são armazenados em uma Blockchain e processados em uma máquina virtual Turing Completa e de uso geral.

6.2 Escopo e desenvolvimento

O Bitcoin e o Ethereum possuem escopo e propósito diferentes. O primeiro se apresenta como uma alternativa ao sistema financeiro tradicional, permitindo a realização de transações de forma segura e não-reversíveis e evitando o gasto duplo, sem a necessidade de entidades financeiras para mediar estas transações. Enquanto o segundo se apresenta como uma sistema econômico que possibilita a execução de contratos inteligentes através de uma linguagem de programação embutida. Assim, apesar de possuir uma unidade de moeda (*ether*), o Ethereum foi projetado para ser um computador descentralizado de uso geral, onde é possível criar e executar aplicações descentralizadas (*DApps*).

Além disso, as duas criptomoedas possuem uma cultura de desenvolvimento diferente. No Bitcoin, o desenvolvimento é guiado por princípios mais conservadores, onde as mudanças são pensadas a fim de evitar que os sistemas existentes não sejam afetados e as alterações sejam compatíveis com as versões anteriores. Entretanto, no Ethereum a cultura de desenvolvimento é

mais focada no futuro e não no passado; logo, se uma mudança é necessária, ela é implementada mesmo que isso signifique invalidar os princípios anteriores, quebrar a compatibilidade entre as versões ou forçar os clientes a atualizarem. (ANTONOPOULOS; WOOD, 2018).

6.3 Funcionamento

As *blockchains* do Bitcoin e do Ethereum funcionam tendo como base a criptografia e a tecnologia de redes *peer-to-peer*. Além disso, em ambas, a Blockchain é uma cadeia de blocos, composta pelas transações e armazenada nos diversos nós da rede.

Por outro lado, elas diferem entre si em alguns pontos. Um aspecto em que o funcionamento das duas criptomoedas se difere é em relação ao algoritmo de consenso. O Bitcoin utiliza o *proof-of-work* (PoW), enquanto o Ethereum utiliza o *proof-of-stake* (PoS). No PoW, os mineradores competem entre si utilizando o seu poder computacional para realizar cálculos e resolver um problema criptográfico. Enquanto o PoS não envolve a realização de cálculos complexos, já que os validadores são selecionados de forma aleatória para validar os blocos e o peso de seus votos têm como base na quantidade de criptomoedas em depósito (*stake*). Além disso, enquanto no PoW o tempo dos blocos possui como base a dificuldade de mineração (no Bitcoin esse tempo é em média 10 minutos), na prova de participação esse tempo é fixo (12 segundos no caso do Ethereum).

De acordo com Pujari et al. (2022) existem algumas vantagens do PoS em relação ao PoW, são elas:

- Melhor eficiência energética – não há necessidade de usar muita energia em cálculos de prova de trabalho.
- Barreiras de entrada mais baixas, requisitos de hardware reduzidos - não há necessidade de possuir um hardware de elite para ter a chance de criar novos blocos.
- Risco de centralização reduzido - a prova de participação deve levar a mais nós protegendo a rede.
- Devido à baixa necessidade de energia, menos emissão de ETH é necessária para incentivar a participação.
- Penalidades econômicas por mau comportamento tornam 51% dos ataques de estilo exponencial mais caros para um invasor em comparação com a prova de trabalho.
- A comunidade pode recorrer à recuperação social de uma cadeia honesta se um ataque de 51% superar as defesas criptoeconômicas.

Entretanto, segundo Pujari et al. (2022) existem algumas desvantagens do PoS em relação ao PoW, são elas:

- A prova de participação é mais jovem e menos testada em comparação com a prova de trabalho.
- A prova de participação é mais complexa de implementar do que a prova de trabalho.
- Os usuários precisam executar três softwares para participar da prova de participação do Ethereum.

6.4 Aspectos financeiros

Existe uma diferença na oferta das duas criptomoedas. O volume máximo de unidades de Bitcoin é 21 milhões, com a taxa de criação diminuindo a cada 4 anos, o que significa que a oferta de novos *bitcoins* vai diminuindo ao longo do tempo. Ao contrário do Ethereum, que não possui um limite máximo de oferta definido, já que a oferta de *ethers* é determinada pelo consenso da rede. Logo, essa oferta pode aumentar ou diminuir dependendo da demanda do mercado.

A Figura 22 apresenta o preço do Bitcoin (em amarelo) e Ethereum (em azul) no período de 2019 a 2023. Nela é possível observar a volatilidade das duas criptomoedas além do preço atual de cada uma, Bitcoin: 16.833,68 USD e Ethereum: 1250,22 USD.

Figura 22 – Preço do Bitcoin e Ethereum de 2019 à 2023 (COINMARKETCAP, 2023)

De acordo com CoinMarketCap (2023), o Bitcoin é a criptomoeda com o maior valor no mercado, enquanto o Ethereum é quarta. Além disso, o Bitcoin e o Ethereum são as criptomoedas com a maior capitalização (*market cap*). Que é o valor total de circulação de uma criptomoeda no mercado, calculado através da multiplicação do valor de uma criptomoeda pelo a oferta

circulante dessa criptomoeda no mercado. Neste caso, o Bitcoin possui um *market cap* que ultrapassa os 360 bilhões de dólares e o Ethereum, 170 bilhões de dólares.

A Figura 23 apresenta um gráfico com as taxas de transação diárias pagas aos mineradores pelo Bitcoin (em azul) e Ethereum (em rosa). O gráfico usa a média móvel de 7 dias.

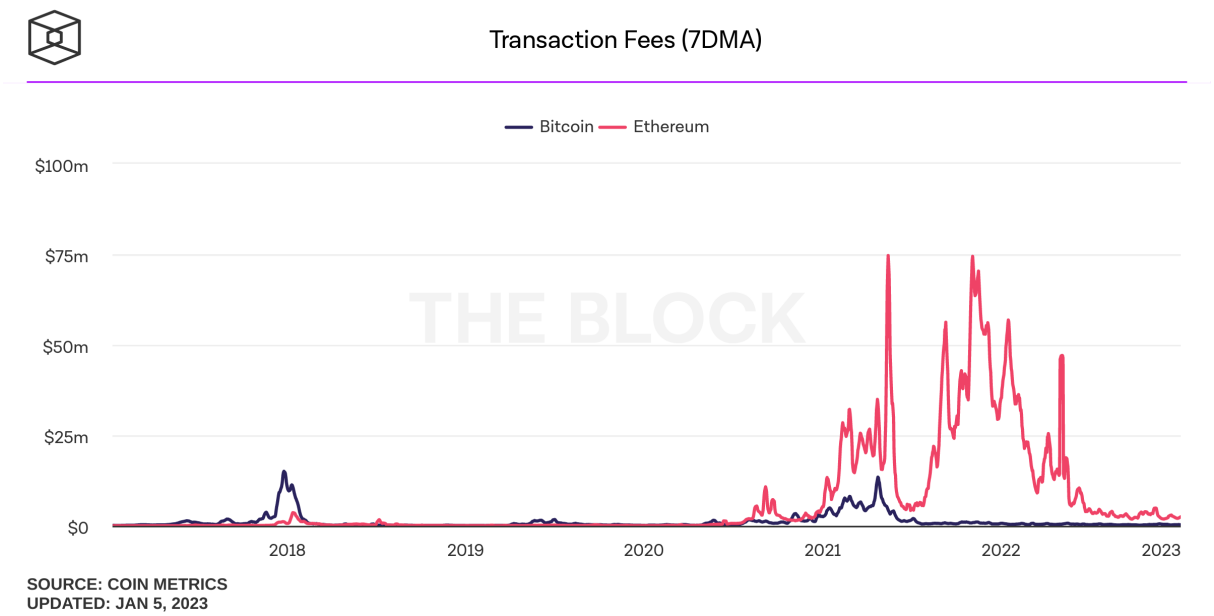

Figura 23 – Taxas de transação (THEBLOCK, 2023)

A Figura 24 apresenta um gráfico com o número de transações por dia do Bitcoin (em azul) e Ethereum (em rosa). O gráfico usa a média móvel de 7 dias.

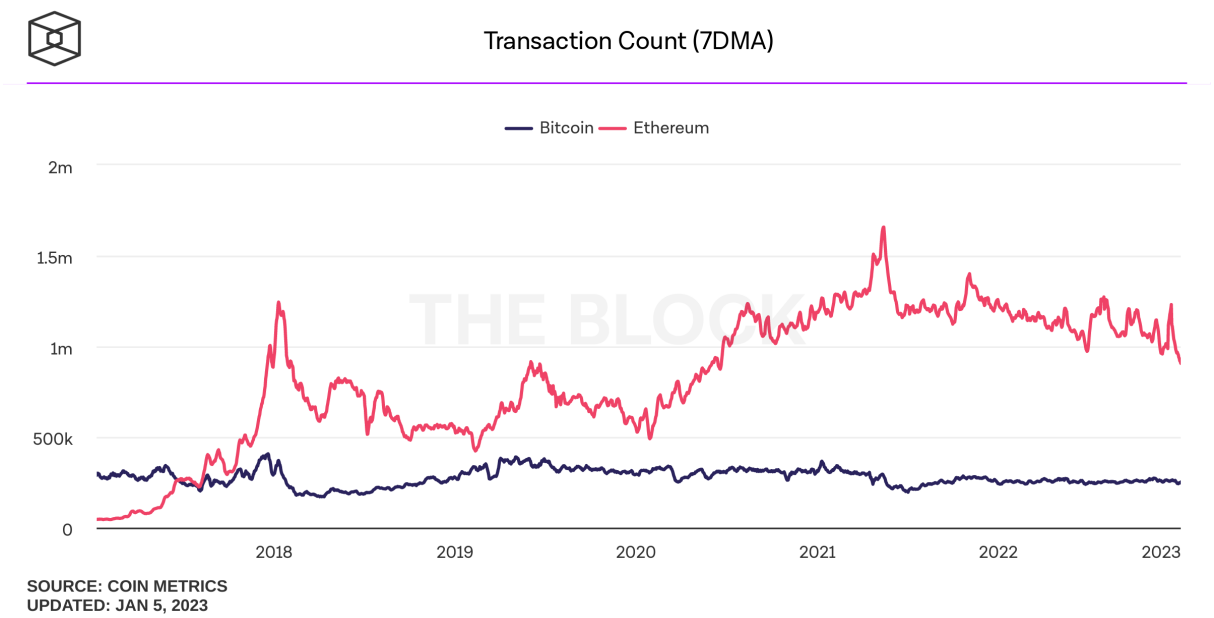

Figura 24 – Número de transações (THEBLOCK, 2023)

A Figura 25 apresenta um gráfico com o número de endereços exclusivos que estavam ativos na rede como remetente ou destinatário no Bitcoin (em azul) e Ethereum (em rosa). Apenas os endereços que estavam ativos em transações bem-sucedidas são contados. O gráfico usa a média móvel de 7 dias.

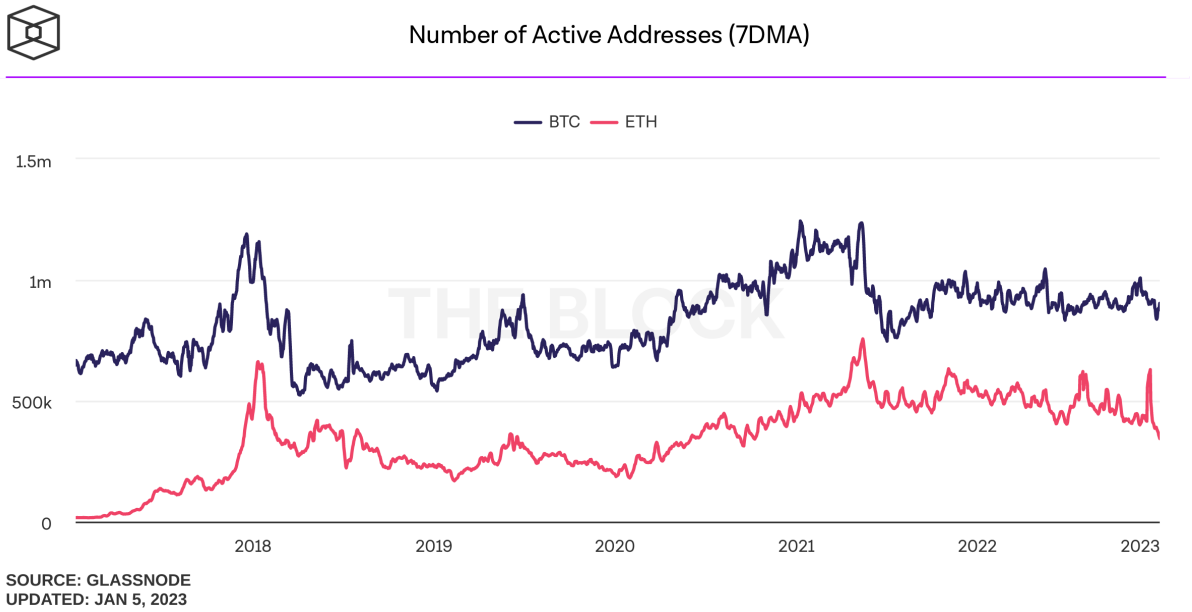

Figura 25 – Número de endereços ativos (THEBLOCK, 2023)

Em resumo, existe uma diferença na oferta das duas criptomoedas, uma vez que o Bitcoin possui um limite máximo de oferta definido e o Ethereum não possui. Além disso, apesar de ambas as criptomoedas apresentarem a maior capitalização do mercado, o Bitcoin possui uma capitalização e valor de mercado consideravelmente mais alto. Porém, é interessante destacar, que o Ethereum possui um maior número de transações e taxas de transação pagas aos mineradores, enquanto o Bitcoin possui um maior número de endereços ativos.

7 Conclusão

O presente trabalho apresentou um estudo sobre a tecnologia Blockchain. Um sistema descentralizado de registro de dados, que possui como componentes as redes *peer-to-peer*, criptografia, entre outros. Atualmente, essa tecnologia é usada em diversas soluções, entre elas, as criptomoedas.

As criptomoedas são moedas digitais alternativas as moedas fiduciárias. Cada uma delas pode possuir uma Blockchain, que é usada para processar e validar as transações do sistema.

O Bitcoin e o Ethereum foram as duas primeiras criptomoedas baseadas na tecnologia Blockchain. Além disso, elas se destacam, como as duas criptos com a maior capitalização do mercado, sendo a capitalização do Bitcoin 360 bilhões de dólares e do Ethereum, 170 bilhões de dólares. Dessa forma, esse trabalho buscou apresentar um estudo sobre a tecnologia Blockchain. além de fazer uma análise comparativa entre essas duas criptomoedas.

O Bitcoin inspirou a criação de várias outras criptomoedas, entre elas o Ethereum. Todavia, enquanto o Bitcoin surge com o propósito de ser um sistema par-a-par de dinheiro eletrônico, o Ethereum surgiu com o propósito de criar contratos inteligentes armazenados em uma Blockchain e processados em uma máquina virtual Turing Completa de uso geral.

As duas criptomoedas possuem algoritmos de consenso distintos, enquanto o Bitcoin utiliza o algoritmo *proof-of-work* (PoW), o Ethereum utiliza *proof-of-stake* (PoS). Ambos possuem vantagens e desvantagens associadas.

Por fim, ambas as criptomoedas apresentam uma diferença de oferta, enquanto o Bitcoin possui um volume máximo de 21 milhões de unidades, o Ethereum não possui um limite máximo de oferta definido. Outros pontos que merecem destaque são as métricas de taxa de transação pagas diariamente, número de transações diárias e número de endereços ativos. Enquanto o Bitcoin possui um maior número de endereços ativos maior, o Ethereum possui um maior número de transações diárias e paga mais taxas aos mineradores diariamente.

Em resumo, ao realizar a análise comparativa foi possível concluir que as duas criptomoedas compartilham de elementos em comum, porém, elas se diferem em alguns aspectos como histórico, escopo, cultura de desenvolvimento, funcionamento e aspectos financeiros. Não sendo o objetivo deste estudo apontar qual das duas criptomoedas é a melhor, mas sim, apontar essas particularidades ao leitor para que ele forme o seu próprio ponto de vista.

7.1 Trabalhos futuros

Algumas sugestões de trabalhos futuros que podem complementar e enriquecer o estudo apresentado incluem: realizar o estudo abordando alguns aspectos com mais profundidade como a economia, legislação e a regulamentação em torno das criptomoedas; realizar um estudo em torno das mudanças e perspectivas para o futuro das criptomoedas; realizar um estudo com a finalidade de comparar os principais protocolos de consenso e realizar um estudo comparativo abordando outras criptomoedas.

Referências

ACDX. *Digital Signature diagram*. 2008. Disponível em https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 9.

ANTONOPOULOS, A. M. *Mastering bitcoin*. [S.l.]: O'Reilly,, 2019. Citado 12 vezes nas páginas xv, 15, 18, 19, 20, 22, 23, 24, 26, 30, 31 e 32.

ANTONOPOULOS, A. M.; WOOD, G. *Mastering ethereum: building smart contracts and dapps*. [S.l.]: O'reilly Media, 2018. Citado 20 vezes nas páginas xv, 14, 15, 16, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49, 50 e 62.

BAPTISTA, S. R. C. *Bitcoin e Blockchain: uma nova classe de ativos*. Tese (Doutorado) — Instituto Universitário de Lisboa, 2019. Citado 12 vezes nas páginas 11, 13, 17, 22, 24, 25, 28, 29, 30, 32, 53 e 56.

BARBOSA, P. C. L. Bitcoin e moedas fiat: Um estudo de volatilidade comparada. *Fundação Instituto de Pesquisas Econômicas–FIPE, São Paulo*, p. 75, 2016. Citado na página 53.

BARCELLOS, A. M. P.; GASPARY, L. P. Segurança em redes p2p: princípios, tecnologias e desafios. In: *Simposio Brasileiro de Redes de Computadores (24.: 2006 maio: Curitiba, PR). Anais dos minicursos. Curitiba:[sn], 2006.* [S.l.: s.n.], 2006. Citado na página 10.

BRANDÃO, P. Criptomoeda: o bitcoin. Universidade Aberta, 2020. Citado 3 vezes nas páginas 11, 12 e 13.

BROCHADO, A. Snapshot da indústria das criptomoedas. *Snapshot da indústria das criptomoedas*, Comissão do Mercado de Valores Mobiliários, n. 59, p. 84–108, 2018. Citado 6 vezes nas páginas 10, 28, 56, 57, 58 e 59.

BURNETT, S. *Criptografia e segurança: o guia oficial RSA*. [S.l.]: Gulf Professional Publishing, 2002. Citado 3 vezes nas páginas 7, 8 e 9.

BUTERIN, V. *A Prehistory of the Ethereum Protocol*. 2017. Disponível em https://vitalik.ca/general/2017/09/14/prehistory.html, acessado em 31 de Outubro de 2022. Citado 2 vezes nas páginas 14 e 15.

BUTERIN, V. et al. Ethereum white paper (2013). *URL https://github.com/ethereum/wiki/wiki/White-Paper*, 2013. Citado 4 vezes nas páginas 35, 37, 42 e 44.

CAVALCANTI, L. R. *Veja os maiores "forks" do mercado de criptomoedas e como estão performando*. 2022. Disponível em https://www.moneytimes.com.br/veja-os-maiores-forks-do-mercado-de-criptomoedas-e-como-estao-performando/, acessado em 16 de Dezembro de 2022. Citado 2 vezes nas páginas 32 e 50.

COINDANCE. *Coin Dance Stats*. 2022. Disponível em https://coin.dance/stats, acessado em 3 de Dezembro de 2022. Citado 2 vezes nas páginas xv e 55.

COINMARKETCAP. *Top 100 Criptomoedas por Capitalização de Mercado*. 2022. Disponível em https://coinmarketcap.com/pt-br/, acessado em 28 de Novembro de 2022. Citado 2 vezes nas páginas xv e 54.

COINMARKETCAP. *CoinMarketCap*. 2023. Disponível em https://coinmarketcap.com/, acessado em 05 de Janeiro de 2023. Citado 3 vezes nas páginas xv, 1 e 63.

COUTINHO, S. Copyright© 2016-2005 by severino collier coutinho direitos reservados, 2016 pela associação instituto nacional de matemática pura e aplicada-impa estrada dona castorina, 110–rio de janeiro–22460-320. 2016. Citado na página 5.

DANNEN, C. *Introducing Ethereum and solidity*. [S.l.]: Springer, 2017. Citado 12 vezes nas páginas 13, 16, 35, 36, 37, 38, 39, 40, 41, 43, 44 e 45.

ETHEREUM.ORG. *The Beacon Chain*. 2023. Disponível em https://ethereum.org/en/upgrades/beacon-chain/, acessado em 20 de Janeiro de 2023. Citado na página 47.

FIGUEIREDO, D. D. Fundamentos em blockchain. 2020. Citado 20 vezes nas páginas 7, 8, 9, 12, 13, 14, 16, 18, 21, 22, 23, 25, 26, 27, 28, 29, 32, 54, 56 e 58.

GANDINI, J. A. D.; SALOMÃO, D. P. d. S.; JACOB, C. A segurança dos documentos digitais. *Disponıvel em< http://www. jus. com. br>. Acesso em: Agosto*, v. 11, 2001. Citado na página 8.

IQ. *Hard forks de ethereum para ficar de olho*. 2018. Disponível em https://www.iq.com.br/investimentos/artigos/hard-forks-ethereum-2, acessado em 16 de Dezembro de 2022. Citado na página 50.

LIMA, M. *Blockchain: O Que É? Como Funciona Essa Tecnologia?* 2020. Disponível em https://criptofy.com/blockchain-o-que-e/, acessado em 19 de Janeiro de 2023. Citado 2 vezes nas páginas xv e 25.

NAIJA, E. *Ethereum 2.0 & The Merge: Everything You Need to Know*. 2022. Disponível em https://eye9ja.com/2022/08/01/ethereum-2-0-the-merge-everything-you-need-to-know/, acessado em 18 de Outubro de 2022. Citado 2 vezes nas páginas xv e 46.

NAKAMOTO, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, p. 21260, 2008. Citado 5 vezes nas páginas xv, 17, 24, 27 e 29.

OKUMURA, M. K. et al. Números primos e criptografia rsa. *Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo*, 2014. Citado na página 5.

OLIVEIRA, R. R. Criptografia simétrica e assimétrica-os principais algoritmos de cifragem. *Segurança Digital [Revista online]*, v. 31, p. 11–15, 2012. Citado 4 vezes nas páginas 5, 6, 7 e 9.

PEREIRA, P. O surgimento das criptomoedas–alteração do paradigma económico. *JANUS 2022-O País Que Somos O(s) Mundo(s) Que Temos: Um roteiro para o conceito estratégico na próxima década*, OBSERVARE. Universidade Autónoma de Lisboa, p. 42–43, 2022. Citado na página 13.

PINTO, P. *Criptografia simétrica e assimétrica. Sabe a diferença?* 2010. Disponível em https://pplware.sapo.pt/tutoriais/networking/criptografia-simetrica-e-assimetrica-sabe-a-diferenca/, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 7.

PUJARI, S. L. R. et al. *PROOF-OF-STAKE (POS)*. 2022. Disponível em https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/, acessado em 18 de Outubro de 2022. Citado 2 vezes nas páginas 47 e 62.

RAUCHS, M.; HILEMAN, G. et al. Global cryptocurrency benchmarking study. *Cambridge Centre for Alternative Finance Reports*, Cambridge Centre for Alternative Finance, Cambridge Judge Business School . . . , 2017. Citado 3 vezes nas páginas 55, 57 e 59.

ROCHA, J. et al. Peer-to-peer: Computaçao colaborativa na internet. In: *Minicursos do XXII Simposio Brasileiro de Redes de Computadores (SBRC 2004)*. [S.l.: s.n.], 2004. Citado na página 10.

RODRIGUES, E. I. *Estudo sobre Bitcoin: escalabilidade da blockchain*. 2016. Citado 8 vezes nas páginas 15, 21, 22, 23, 28, 29, 31 e 32.

SAKURAI, R. G. *Criptografia de chave privada - Simétrica*. 2020. Disponível em http://www.universidadejava.com.br/outros/criptografia-simetrica/, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 6.

SALEH, F. Blockchain without waste: Proof-of-stake. *The Review of financial studies*, Oxford University Press, v. 34, n. 3, p. 1156–1190, 2021. Citado na página 47.

SANTOS, C. Tecnologia blockchain: Uma proposta de implementação na universidade federal do tocantins. Universidade Federal do Tocantins, 2018. Citado 7 vezes nas páginas 6, 7, 9, 10, 17, 25 e 27.

SICHEL, R. L.; CALIXTO, S. R. Criptomoedas: impactos na economia global. perspectivas. *Revista de Direito da Cidade*, v. 10, n. 3, p. 1622–1641, 2018. Citado 4 vezes nas páginas 10, 16, 17 e 53.

SILVA, J. d. O.; MACHADO, L. G. L. Moedas digitais bitcoin. Universidade Federal Fluminense, 2017. Citado 2 vezes nas páginas 10 e 13.

SOARES, E. C. *Os fundamentos das cripto moedas*. Tese (Doutorado), 2021. Citado na página 53.

SOUZA, C. M. d. Um estudo do funcionamento da criptografia simétrica e assimétrica como ferramenta de segurança computacional em redes locais e na web. *Incubadora De Empresas: Instrumento Para a Competitividade das*, p. 242, 2008. Citado na página 7.

THEBLOCK. *Comparison Bitcoin and Ethereum*. 2023. Disponível em https://www.theblock.co/data/on-chain-metrics/comparison-bitcoin-ethereum, acessado em 05 de Janeiro de 2023. Citado 3 vezes nas páginas xv, 64 e 65.

TRADINGECONOMICS. *Trading Economics*. 2022. Disponível em https://tradingeconomics.com/, acessado em 3 de Dezembro de 2022. Citado 3 vezes nas páginas xv, 56 e 57.

VERGARA, S. C. Tipos de pesquisa em administração. Escola Brasileira de Administração Pública da FGV, 1990. Citado na página 3.

WAN, S. *Internet vs. crypto adoption chart predicts 1 billion users by 2027*. 2021. Disponível em https://cryptoslate.com/internet-vs-crypto-adoption-chart-predicts-1-billion-users-by-2027/, acessado em 18 de Outubro de 2022. Citado 2 vezes nas páginas xv e 54.

WANDER, M. *Bitcoin Address*. 2013. Disponível em https://commons.wikimedia.org/wiki/File:Bitcoin_Address.svg, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 21.

WANDER, M. *Bitcoin Block Data*. 2013. Disponível em https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.svg, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 27.

WANDER, M. *Bitcoin Transaction Inputs and Outputs*. 2013. Disponível em https://commons.wikimedia.org/wiki/File:Bitcoin_Transaction_Inputs_and_Outputs.png, acessado em 11 de Outubro de 2022. Citado 2 vezes nas páginas xv e 23.