LIGA DO MERCADO FINANCEIRO
DESDE 2015

Criptoativos

Um curso produzido pela equipe de Educação Financeira da Liga do Mercado Financeiro da Unicamp

ÍNDICE

Capítulo 1 - O que São Criptoativos ..... Página 03

1.1 - Blockchain

1.2 - Movimento Cypherpunk

Capítulo 2 - Bitcoin ..... Página 07

2.1 - O que é Bitcoin ?

2.2 - Propriedades e Funcionamento

2.3 - Problemas de Escalabilidade e Energia

Capítulo 3 - Ethereum ..... Página 12

3.1 - Origem

3.2 - Propriedades e Funcionamento

3.3 - Proof of Work

3.4 - Ethereum 2.0

Capítulo 4 - Altcoins ..... Página 15

4.1 - O que são ?

4.2 - Como surgiram as Altcoins ?

4.3 - Qual sua Funcionalidade ?

4.4 - E os outros Ativos Digitais ?

Capítulo 5 - Ethereum Killers ..... Página 17

5.1 - O que são ?

5.2 - Quais as principais características da “Ethereum Killers?”

5.3 - Exemplos das “Ethereum Killers”

ÍNDICE

Capítulo 6 - Solana: A maior Ethereum Killer ..... Página 21

6.1 - O que é ?

6.2 - Inovação à Blockchain

6.3 - Solana x Ethereum

6.4 - Críticas à rede da Solana

6.5 - Comparativo em relação a Ethereum

Capítulo 7 - Porque Investir no Setor ..... Página x

7.1 - Inovações

7.2 - Empresas e Governos

7.3 - Espaço de crescimento do setor

7.4 - Potencial do Bitcoin como moeda reserva

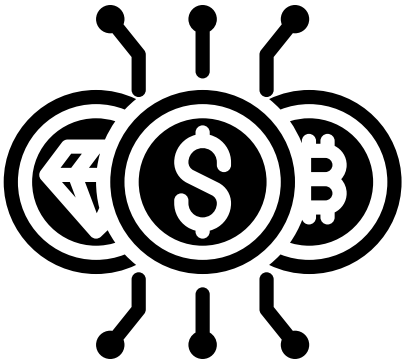
Capítulo 8 - Como Investir no Setor ..... Página x

8.1 - Escolhendo a plataforma certa

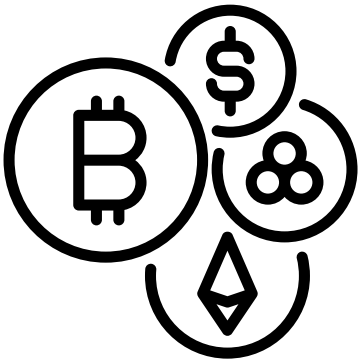
8.2 -Analisando o Mercado: Métricas e Ferramentas

CAPÍTULO 1 - O QUE SÃO CRIPTOATIVOS

CRIPTOATIVOS



Em resumo, criptoativos são **ativos digitais de valor direto ou indireto** armazenados e protegidos por uma **rede descentralizada** chamada **Blockchain**, que será abordada mais adiante. Devido à sua segurança, proporcionada pela criptografia e pela ausência de intermediários como bancos ou governos, eles têm ganhado destaque como forma de investimento, apesar dos riscos e volatilidade associados com o setor.



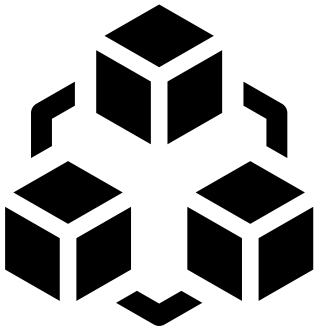
Há diversos tipos de criptoativos, cada um com um propósito distinto. Um exemplo são as **criptomoedas**, que funcionam como moedas digitais usadas em transações no ambiente virtual. Ao contrário das moedas tradicionais, como o real ou o dólar, não são emitidas por governos ou bancos centrais, mas por redes descentralizadas baseadas na tecnologia de Blockchain

PARA QUE SERVEM ?

Os criptoativos possuem diversos propósitos, e as pessoas começam a estudá-los conforme suas necessidades. Podemos destacar algumas de suas finalidades, como **investimentos**, onde muitos investidores buscam criptomoedas como forma de aumentar seu patrimônio rapidamente, aproveitando-se da volatilidade do setor; **Método de pagamento**, uma vez que, em alguns países e ambientes digitais, servem como alternativa à opções existentes; **Governança**, já que alguns criptoativos concedem aos detentores o direito de votar em decisões importantes relacionadas ao desenvolvimento e à operação de uma rede blockchain específica; E, por fim, **a tokenização de ativos**, na qual certos ativos, físicos ou digitais, podem ser divididos em partes (tokens), facilitando suas transações e aumentando sua liquidez.

1.1 BLOCKCHAIN

Agora será explicado como funcionam as redes nas quais esses ativos são gerados e armazenados, a Blockchain. Blockchain é essencialmente uma **tecnologia** que consiste em uma grande **rede de dados**, permitindo o compartilhamento **transparente** das informações armazenadas. Todo e qualquer criptoativo está inserido em uma Blockchain, o que possibilita a visualização de todas as transações realizadas e dos envolvidos, porém, utilizando **pseudônimos** para preservar a identidade dos participante



COMO FUNCIONAM ?

Uma Blockchain funciona baseada em 3 princípios: **Imutabilidade, Consenso e Descentralização,** garantindo assim uma rede segura e confiável para o registro de transações, permitindo que os dados sejam protegidos contra alterações, enquanto assegura que todos os participantes da rede concordem com as informações registradas. Além disso, sua estrutura elimina a necessidade de uma autoridade central, promovendo maior segurança e transparência no processo.

1 IMUTABILIDADE

A **Imutabilidade** da rede consiste em que qualquer coisa que foi adicionada ao Blockchain não poderá ser mudado por ninguém, ele ficará para sempre registrado naquele rede, se essa imutabilidade for perdida a rede será corrompida.

2 CONSENSO

O **Consenso** é o processo fundamental que garante a validação e a concordância entre os participantes de uma rede Blockchain, permitindo que uma transação seja aceita. Cada rede tem seu próprio tipo de **mecanismo de consenso**, que define regras para quem e quantos podem/devem votar. Isso é **extremamente importante**, pois determina quão segura a rede é, assim como sua eficiência energética, escalabilidade e descentralização.

3 DESCENTRALIZAÇÃO

A **Descentralização** significa que, ao contrário dos sistemas tradicionais em que um banco de dados é controlado por uma única entidade (como um banco ou governo), o Blockchain é mantido por uma rede de computadores (nós) que operam de forma conjunta. Garante que a rede continuará a funcionar de forma segura mesmo que alguns nós deixem de funcionar, ou sejam corrompidos por criminosos.

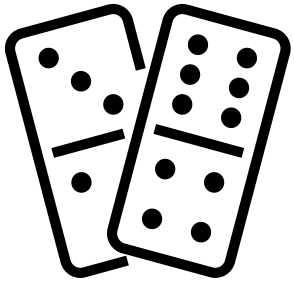
COMPARAÇÃO

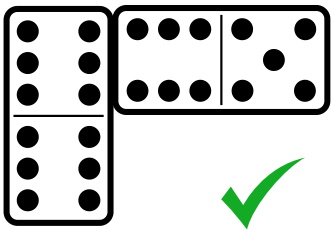
Para simplificar o funcionamento de uma rede blockchain, podemos compará-la a um **jogo de dominó**.

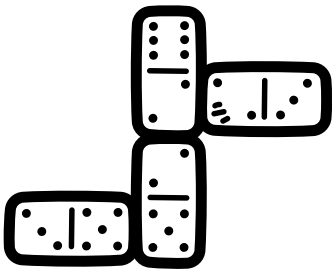
A **descentralização** é semelhante a cada jogador ter suas próprias peças; mesmo que alguém saia do jogo, os outros podem continuar jogando.

O **consenso** se refere ao fato de que, para colocar uma peça no jogo, todos os jogadores devem concordar que a jogada segue as regras do dominó

A **imutabilidade** é representada pelo princípio de que, uma vez que uma peça é colocada no jogo, ela não pode mais ser removida, e todos os jogadores podem vê-la.





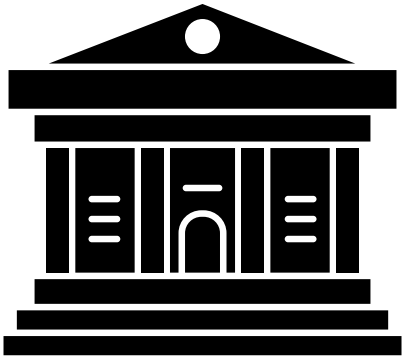


1.2 MOVIMENTO CYPHERPUNK

Com a grande explosão do mundo digital nos últimos anos, várias pessoas absorveram as ideias dos criptoativos e defendem os seus valores, e encaram esse **"novo mundo"** como o futuro. Esse movimento teve início em meados dos anos 90, na Califórnia, mais especificamente na região chamada Silicon Valley ou **Vale do Silício**, principal região de produção tecnológica dos Estados Unidos. Lá vários profissionais de empresas de tecnologia se reuniram em blogs para disseminar a **ideia dos criptoativos**, por estarem preocupados com a **privacidade**, **liberdade** e **anonimato** no ambiente digital. Esse movimento ficou conhecido como movimento **Cypherpunk**, onde "cypher" se refere à criptografia e "punk" em referência ao espírito rebelde.

Os cypherpunks se baseiam em alguns pilares, em que defendem a **privacidade**, a **liberdade individual** e a **desconfiança em relação à autoridade**, utilizando a **criptografia** como ferramenta principal. Os cypherpunks acreditam que a privacidade é um direito fundamental, que deve ser protegido contra a vigilância crescente por parte de governos e corporações. Para eles, a criptografia é o meio mais eficaz para garantir essa privacidade, permitindo que as pessoas **protejam suas comunicações** e **transações de interceptações indesejadas**. Além disso, o movimento valoriza profundamente a **liberdade individual**, defendendo que cada pessoa deve ter o controle sobre suas informações e a capacidade de se expressar e transacionar **sem interferência externa**.

A **desconfiança em relação à autoridade** é outro aspecto central, pois os cypherpunks veem governos e instituições de poder com **ceticismo**, especialmente no que tange à **vigilância** e ao **controle das atividades online**. Por isso, eles promovem o desenvolvimento de tecnologias descentralizadas, que evitam a concentração de poder e garantem a segurança e a autonomia dos indivíduos. Esses pilares guiaram não apenas as discussões filosóficas e políticas do movimento, mas também influenciaram diretamente o **desenvolvimento de tecnologias** que hoje são fundamentais para a privacidade e a liberdade digital, como o **Bitcoin** e outros sistemas de criptomoedas



FATOS HISTÓRICOS DO MOVIMENTO

A primeira ação registrada dos cypherpunks seria a "**Cypherpunk Mailing List**", uma plataforma de debates entre programadores que defendiam a **liberdade** e a **privacidade do mundo digital**, além de discutir sobre métodos de criptografia e programação. Entre as principais figuras que contribuíram para a plataforma estavam indivíduos como **Tim May** e **John Gilmore**. Eles, junto com outros, contribuíram para o desenvolvimento e propagação de ideias e tecnologias inovadoras. Tim May, por exemplo, foi o autor de "**The Crypto Anarchist Manifesto**", que imaginou um mundo onde a criptografia emanciparia os indivíduos da vigilância e do controle de governos e corporações

Outro ponto histórico do movimento foi em 1993, **Eric Hughes**, um matemático, programador e um líder do movimento cypherpunk publicou o **Manifesto Cypherpunk**, explicitando as ideias que dão base nesse pensamento, sendo traduzido como "A privacidade é necessária para termos uma sociedade aberta na era eletrônica. Privacidade não é o mesmo que segredo. Um assunto privado é uma coisa que alguém não quer que o mundo inteiro saiba; um assunto secreto é uma coisa que alguém não quer que ninguém saiba. A privacidade é o poder de revelar-se seletivamente para o mundo", em um dos seus trechoS

CAPÍTULO 2 – BITCOIN

2.1 O QUE É BITCOIN ?

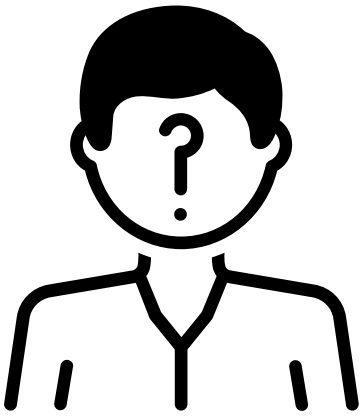
Após a apresentação dos conceitos de criptoativos e suas funções, será abordado o Bitcoin, a criptomoeda mais conhecida globalmente. O **Bitcoin** é uma moeda digital **descentralizada**, criada em 2008. Operando **sem a necessidade de intermediários** como bancos ou governos, o Bitcoin utiliza uma rede de blockchain para registrar todas as transações de forma transparente e segura. Sua principal característica é a **escassez**, com um limite de 21 milhões de unidades, o que o diferencia das moedas tradicionais que podem ser impressas em quantidade ilimitada. Ao longo dos anos, o Bitcoin tornou-se a **criptomoeda mais conhecida** e amplamente adotada, tanto como reserva de valor quanto como meio de troca em algumas transações.

BACKGROUND HISTÓRICO

Em 2008 ocorreu a **crise do mercado imobiliário**, também conhecida como a Crise do Subprime, que foi desencadeada pelo **colapso do mercado imobiliário nos Estados Unidos**. Bancos concediam empréstimos hipotecários de alto risco (subprime) para pessoas com baixa capacidade de pagamento, alimentando uma bolha imobiliária. Quando os mutuários começaram a inadimplência, o valor dos imóveis despencou, levando à **falência grandes instituições financeiras** e gerando uma **crise de confiança** nos mercados globais. A crise resultou em uma profunda **recessão mundial**, com impacto severo no emprego, na economia real e no sistema bancário, exigindo resgates governamentais para estabilizar a economia

MOTIVAÇÃO

Com toda essa situação, **Satoshi Nakamoto** estava irritado com o jeito que a economia andava e de como o Estado tinha uma grande influência no nosso sistema financeiro, e também ele fazia parte do **Movimento Cypherpunk** e era um membro ativo nos blogs, defendendo a ideia de descentralização da economia. Portanto, no dia 31 de outubro de 2008 Satoshi Nakamoto enviou o **whitepaper do Bitcoin** para uma série de membros importantes do Movimento Cypherpunk e do mundo da criptografia, dando início a uma **revolução digital**.



CRIADOR

Utilizando um pseudônimo, até hoje ninguém sabe com certeza seu nome real, ou se "Nakamoto" representa uma única pessoa ou um grupo. Após publicar o whitepaper, Nakamoto permaneceu ativo no desenvolvimento do software até 2010, quando se afastou alegando que iria "se dedicar a outros projetos". Estima-se que ele possua mais de **1 milhão de bitcoins**, uma quantia que nunca foi movimentada desde a criação da criptomoeda e que, se convertida, ultrapassa o valor de **50 bilhões de dólares**. Embora várias tentativas tenham sido feitas para revelar sua verdadeira identidade, **todas falharam**.

WHITEPAPER

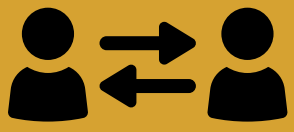
O **whitepaper do Bitcoin** é um documento de nove páginas que apresenta a visão de Nakamoto para um **sistema de pagamento descentralizado** que permite transações diretas entre partes **sem a necessidade de intermediários**, como bancos ou instituições financeiras, que foi disponibilizado em 2008. Esse documento trazia todas as principais informações do funcionamento da criptomoeda. Ela era armazenada numa rede **Blockchain**, com cada bloco contendo um conjunto de transações, um carimbo de data e hora, e um link para o bloco anterior, formando uma **cadeia imutável**. Satoshi ainda criou a **transação P2P** (peer to peer), onde não há a necessidade de terceiros ou uma autoridade para validar a transação, conquistando assim a tal sonhada **descentralização** de sua criptomoeda. Embora as transações sejam públicas, os usuários são identificados por chaves criptográficas, garantindo um certo **grau de anonimato**, porém com a transparência de cada transação.

ESCASSEZ PROGRAMADA

O Bitcoin tem um número máximo de **21 milhões de unidades**, o que traz um certo valor potencial como reserva de futuro.

PEER TO PEER (P2P)

o sistema de transações **P2P** elimina a necessidade de intermediários, garantindo **descentralização** e transparência nas transações



Sem a necessidade de um terceiro para validar as transações, como garantir que todas elas seriam legítimas?

PROOF OF WORK

2.2 PROPRIEDADES E FUNCIONAMENTO

PROOF OF WORK (POW)

Esse mecanismo é essencial para adicionar **novos blocos à Blockchain**. Na prática, os mineradores competem entre si resolvendo **cálculos matemáticos complexos**. Ao encontrar a solução correta, chamada ***nonce***, o minerador gera um ***hash***, uma sequência de caracteres criptográficos que segue um padrão específico, geralmente começando com um determinado número de zeros

Quando o minerador encontra o *nonce* correto, ele submete a "prova de trabalho" à rede, validando o bloco e ganhando o direito de **adicioná-lo à blockchain**. Como recompensa, o minerador **recebe Bitcoins** e as taxas das transações contidas no bloco. Esse processo, que ocorre aproximadamente a cada **10 minutos**, é computacionalmente intensivo, tornando o sistema **resistente a manipulações**. Além disso, a dificuldade dos cálculos ajusta-se automaticamente conforme mais mineradores entram na rede, garantindo o **equilíbrio** e a **segurança** contínua do sistema.

Resolver um **cubo mágico** é semelhante a encontrar o nonce correto no **PoW**. Ambos envolvem uma **tentativa e erro complexa**: no cubo mágico, você precisa manipular as faces e as combinações de peças até **alcançar a solução correta**. Da mesma forma, no PoW, os mineradores tentam diversas combinações de números até encontrarem um *nonce.*

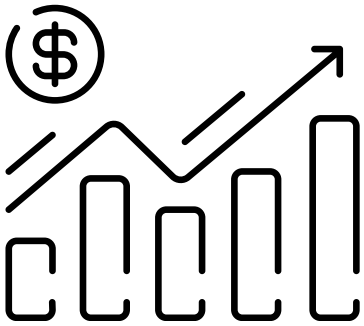
Além disso, uma vez que a solução é encontrada, verificar sua correção é relativamente **simples**. No cubo mágico, você pode facilmente confirmar se todas as faces estão na **cor certa**. No PoW, a rede pode rapidamente verificar se o *hash* gerado atende aos **critérios necessários**

TOKENOMICS

É a **estrutura econômica** e o **funcionamento** dos tokens da criptomoeda, englobando como eles são distribuídos, utilizados e como seu valor é **influenciado**. O modelo de ***tokenomics*** do Bitcoin também contribui para sua **valorização**, já que com uma oferta limitada e a redução periódica na criação de novos bitcoins, potencialmente aumenta o valor da criptomoeda. Esse modelo deflacionário é projetado para criar uma economia onde a **oferta reduzida** e a **demanda crescente** possam **impulsionar o preço**. Além disso, este modelo de *tokenomics* garante que a rede permaneça **segura** e **descentralizada** pois a recompensa pela mineração e a validação das transações incentivam a participação dos mineradores e ajudam a **evitar a centralização do controle da rede**, alinhando os incentivos econômicos com a integridade da blockchain.

HALVING

Durante o **Halving**, a recompensa por minerar um bloco é reduzida pela **metade**, o que diminui a quantidade de **novos bitcoins** que entram em circulação. O Halving não apenas controla a oferta de novos bitcoins, mas também **aumenta a dificuldade da mineração** ao longo do tempo, uma vez que o valor da recompensa está diminuindo. Esse mecanismo é fundamental para o **modelo deflacionário** do Bitcoin, ajudando a garantir que a oferta total de bitcoins seja atingida de maneira **gradual e previsível**. Além disso, o Halving tende a impactar o preço do Bitcoin, uma vez que a **redução na oferta** em relação à demanda, tende a **aumentar** o valor da criptomoeda.



No futuro, à medida que a recompensa por bloco se aproxima de zero e todos os bitcoins forem minerados, a rede dependerá principalmente das taxas de transação para compensar os mineradores. Esse modelo de longo prazo assegura que a segurança da rede continue mesmo quando a criação de novos bitcoins chegar ao fim. A *tokenomics* do Bitcoin, portanto, é projetada para criar um sistema econômico sustentável e seguro, alinhando os incentivos com a estabilidade e integridade da rede.

2.3 PROBLEMAS DE ESCALABILIDADE E ENERGIA

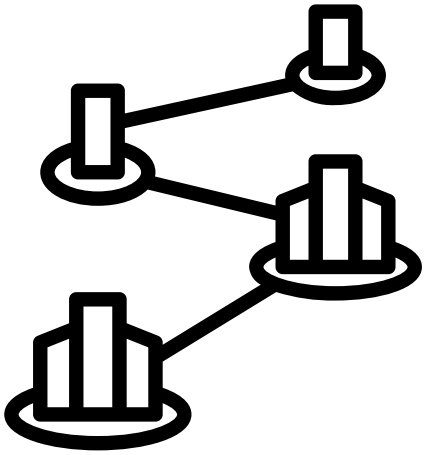
Embora o sistema do Bitcoin seja extremamente **seguro** e **descentralizado**, ele enfrenta desafios significativos, sendo a **escalabilidade** um dos principais. Esse problema está relacionado à capacidade da rede de processar transações, especialmente em blockchains que utilizam o mecanismo proof-of-work. Por ser **computacionalmente intensivo**, o proof-of-work não apenas torna o processamento de transações **mais lento,** mas também resulta em um **consumo energético elevado**, afetando a **eficiência** do sistema.

ESCALABILIDADE

A escalabilidade refere-se à capacidade de uma rede de processar um **grande volume** de transações rapidamente e de maneira **eficiente** à medida que o número de usuários e transações **aumenta**. Esse fator é crucial porque impacta diretamente a **velocidade**, o **custo** e a **capacidade geral** da rede. No caso do Bitcoin, a capacidade de processamento é limitada a aproximadamente **7 transações por segundo (TPS)** e há um intervalo de cerca de **10 minutos** entre a validação e a criação de um novo bloco. Para efeito de comparação, uma empresa global de serviços financeiros, como a ***Mastercard Inc*** registrou um total de **5.000 TPS** no último ano, e no caso da ***Visa***, seu diretor financeiro Vasant Prabhu, disse que a rede poderia lidar, em teoria, com **65.000 TPS.**

AUMENTO DE DEMANDA

Com o aumento da demanda, a rede do Bitcoin pode enfrentar **congestionamentos**, resultando em **transações mais lentas** e **taxas mais altas**. À medida que mais pessoas utilizam a criptomoeda, a quantidade de transações a serem processadas cresce, e se a rede não for suficientemente escalável, ela se torna **sobrecarregada**. Isso provoca atrasos na confirmação das transações e eleva as taxas de transação, pois os usuários pagam mais para garantir que suas transações sejam processadas mais **rapidamente**.



CONSUMO ENERGÉTICO

Outro grande problema da rede Bitcoin é o **alto consumo de energia** necessário para que os mineradores encontrem, resolvam e adicionem novos blocos à blockchain. O processo de Proof of Work, exige uma **quantidade desmedida de poder computacional**, resultando em um gasto energético **extremamente elevado**. À medida que as recompensas pela mineração diminuem devido ao Halving, o incentivo econômico para os mineradores também **diminui**, o que pode reduzir a participação no processo de mineração. Para efeito de comparação, o Bitcoin consome anualmente cerca de 130,9 terawatt-horas (TWh) de energia, superando o **consumo total da Argentina**, que utiliza aproximadamente 125,03 TWh por ano.

IMPACTO AMBIENTAL

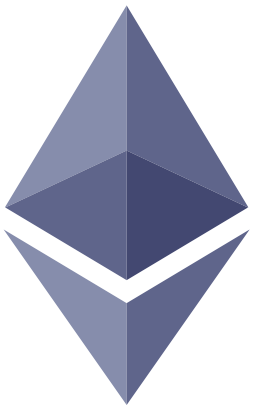
O **impacto ambiental** desse consumo energético é um fator de crescente **preocupação**. Grande parte da energia utilizada pelos mineradores provém de **fontes não renováveis**, o que contribui para emissões significativas de carbono. Isso coloca o Bitcoin em conflito com os esforços globais para **reduzir as pegadas de carbono e mitigar as mudanças climáticas**. Além disso, à medida que a dificuldade da mineração aumenta, mais recursos computacionais são exigidos, intensificando o **problema ambiental**

Sendo assim o sistema do Bitcoin é **bem complexo**, com novas tecnologias para garantir a tão sonhada **descentralização** de Satoshi Nakamoto. Além de ter um grande plano para continuar sobrevivendo ao longo prazo, respeitando as suas barreiras e contando com a participação de pessoas do mundo inteiro para continuar a manutenção de sua rede

CAPÍTULO 3 - ETHEREUM

3.1 O QUE É ETHEREUM?

Ethereum é uma plataforma descentralizada baseada em blockchain que permite a criação e execução de contratos inteligentes (smart contracts) e aplicações descentralizadas (dApps). Lançada em 2015, ela utiliza a criptomoeda Ether (ETH) como combustível para suas operações. Ao contrário do Bitcoin, que é focado em ser uma moeda digital, o Ethereum é mais voltado para fornecer uma infraestrutura flexível para desenvolver e implementar uma ampla gama de aplicativos e serviços financeiros, como DeFi (Finanças Descentralizadas) e NFTs (Tokens Não Fungíveis).



WHITEPAPER

Um whitepaper é um documento técnico que explica, de forma detalhada, uma proposta, conceito ou solução para um problema específico.
É usado principalmente para apresentar produtos, serviços, tecnologias ou políticas, objetivando educar, fornecer uma visão clara sobre o tema e persuadir potenciais interessados ou investidores.

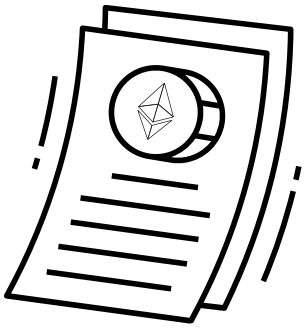
ORIGEM

VITALIK BUTERIN
criador e idealizador do Ethereum

Vitalik Buterin, nascido em 1994, é um programador e escritor russo-canadense que começou a se envolver com o mundo das criptomoedas bem cedo, ainda como adolescente. Em 2011, ele cofundou a Bitcoin Magazine, onde passou a escrever sobre o potencial do Bitcoin e da tecnologia blockchain, o que o tornou uma figura conhecida na comunidade. No entanto, ao se aprofundar no Bitcoin, ele logo identificou uma limitação fundamental, levando-o a, em 2013, lançar o Whitepaper da rede Ethereum.

PROPOSTA

A limitação encontrada por Vitalik no Bitcoin era a sua funcionalidade bastante **restrita a transações simples**. Para Vitalik, a tecnologia da blockchain tinha o potencial de ser usada para **muito mais do que apenas transações financeiras**.
Dessa forma ele imaginou uma plataforma que pudesse alavancar a blockchain para casos de uso mais complexos, como a **execução de contratos de forma autônoma e descentralizada**, sem a necessidade de intermediários.
Esse conceito foi introduzido como ***smart contracts***, e viriam a permitir que a tecnologia se expandisse para diversas indústrias através da criação de ***dapps.***



3.2 O QUE SÃO SMART CONTRACTS?

Um smart contract é, na essência, **um programa que roda em uma blockchain**. Ele tem a capacidade de **verificar, executar e reforçar automaticamente os termos de um acordo digital**. Por exemplo, imagine que você deseja alugar um apartamento usando um smart contract. O contrato poderia estar programado para liberar a chave digital do apartamento para o inquilino assim que o pagamento for recebido. Uma vez que o pagamento é feito, o smart contract automaticamente concede o acesso, sem a necessidade de um intermediário como uma imobiliária ou banco. A maior vantagem é que os smart contracts são transparentes e imutáveis, pois tudo é registrado na blockchain e não pode ser alterado após sua criação. Isso garante segurança e confiança entre as partes envolvidas.

CASOS DE USO

Os smart contracts trouxeram uma nova era de inovação, permitindo que a blockchain fosse usada em uma ampla gama de aplicações que antes seriam inviáveis ou extremamente burocráticas. Aqui estão alguns exemplos detalhados de como os smart contracts podem ser aplicados:

Finanças Descentralizadas (DeFi) 1

Uma das maiores inovações trazidas pelos smart contracts é o crescimento das finanças descentralizadas, ou DeFi. Aplicações DeFi permitem que pessoas realizem empréstimos, negociações e investimentos sem a necessidade de um banco ou corretora. Por exemplo, um contrato inteligente pode permitir que uma pessoa deposite ativos digitais como garantia, obtenha um empréstimo instantaneamente e receba seus ativos de volta assim que o empréstimo for pago — tudo isso sem a necessidade de um intermediário humano.

Exemplo DEFI

Uniswap (UNI)
- Uma das maiores exchanges descentralizadas (DEXs), permite a votação em mudanças de protocolos e decisões importantes

2 *NFT's (Non-Fungible Tokens)*

Os NFTs (Non-Fungible Tokens) são tokens digitais exclusivos que utilizam a tecnologia blockchain para representar a propriedade de um ativo específico e não replicável. Ao contrário das criptomoedas como Bitcoin ou Ethereum, que são fungíveis (ou seja, cada unidade é idêntica e intercambiável), os NFTs são não fungíveis, o que significa que cada um deles é único e não pode ser substituído por outro de igual valor. Uma funcionalidade interessante especulada por alguns seria a emissão de um RG digital.

Exemplo NFT's

Bored Ape Yacht Club (BAYC)
- São 10.000 imagens únicas de macacos desenhados em estilo cartoon, sendo as mais valiosas se tornando um **símbolo de status**.

Gestão da Cadeia de Suprimentos 3

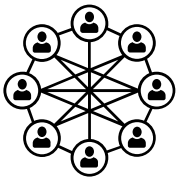
Empresas podem usar smart contracts para automatizar o monitoramento de produtos ao longo da cadeia de suprimentos. Imagine que um produto esteja sendo transportado e precisa passar por vários checkpoints. Cada vez que o produto chega a um checkpoint, essa informação pode ser registrada na blockchain automaticamente e se o produto não chegar dentro do prazo, o contrato pode acionar penalidades ou notificações, garantindo a responsabilidade de todos os envolvidos.

Exemplo SC

VeChain (VET)
- Lidera o setor e é amplamente adotada em várias indústrias. Dentre as suas parcerias destacam-se: Walmart China e BMW.

3.3 PROPRIEDADES DA REDE

Abaixo serão abordadas algumas das propriedades que garantem o funcionamento da rede Ethereum:



DESCENTRALIZAÇÃO

A Ethereum opera em uma rede de nós distribuídos, que mantêm a integridade da rede sem necessidade de uma autoridade central, proporcionando resistência a censura e segurança.

SMART-CONTRACTS

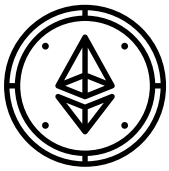
A Ethereum foi pioneira na implementação de contratos inteligentes, que são programas autônomos que executam automaticamente comandos de acordo com condições pré-definidas. Isso viabiliza acordos e transações automáticas, eliminando intermediários.

ETHEREUM VIRTUAL MACHINE (EVM)

É um ambiente de execução virtual que permite que desenvolvedores executem códigos, principalmente na linguagem Solidity. É nele que os smart-contracts são executados.

TOKENIZAÇÃO E CRIAÇÃO DE ATIVOS

A Ethereum permite a criação de tokens baseados em padrões como ERC-20 (para tokens fungíveis) e ERC-721 (para tokens não fungíveis, ou NFTs). Isso facilita a criação de diversos tipos de ativos digitais, como criptomoedas, NFTs, entre outros.

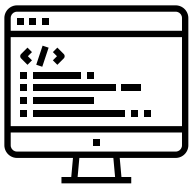


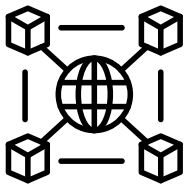
SEGURANÇA E CONSENSO

Desde a atualização Ethereum 2.0, a rede passou do mecanismo de consenso Proof of Work (PoW) para Proof of Stake (PoS), o que reduz o consumo energético e possibilita maior escalabilidade e segurança.

PROGRAMABILIDADE

Diferente do Bitcoin, a Ethereum é programável, possibilitando o desenvolvimento de aplicativos personalizados que podem realizar uma ampla variedade de operações, não se limitando a transações financeiras.





INTEROPERABILIDADE

A Ethereum é compatível com outras blockchains, especialmente com a ajuda de sidechains e soluções de segunda camada. Isso permite a transferência de ativos e informações entre redes diferentes.

3.4 TOKENOMICS DA REDE

O tokenomics da Ethereum abrange a estrutura econômica e de governança dos tokens da rede, focando principalmente no fornecimento, uso, emissão e políticas de valorização dos tokens ETH. Com a atualização do Ethereum 2.0 e a implementação da Proposta de Melhoria da Ethereum (EIP-1559), várias mudanças ocorreram na forma como os tokens ETH são emitidos, utilizados e queimados. Abaixo estão os principais elementos do tokenomics da Ethereum:

OFERTA

Diferente do Bitcoin, a Ethereum **não tem um limite máximo fixo de tokens**, mas a **EIP-1559** e a transição para **Proof of Stake (PoS)** ajudam a controlar o crescimento da oferta total de ETH. **A EIP-1559** introduziu um **mecanismo de queima** de parte das **taxas** de transação, removendo ETH da circulação. Esse mecanismo **reduz a oferta total** de ETH, especialmente em períodos de **alta demanda**, quando **mais tokens são queimados** do que criados. Com o **Proof of Stake** validadores que travam ETH na rede recebem recompensas por validar transações, essas **recompensas variam conforme a quantidade total de ETH em staking**: **mais ETH** em staking **reduz as recompensas individuais** e, assim, a **inflação** de ETH.

EIP-1559

A EIP-1559 (Ethereum Improvement Proposal 1559) é uma das melhorias mais significativas para a rede Ethereum, introduzida com a atualização London em agosto de 2021. Ela reformulou o mecanismo de taxas de transação (gas fees) na rede, buscando melhorar previsibilidade de taxas, experiência dos usuários e eficiência de uso de recursos.

Antes da EIP-1559, a rede Ethereum operava com um sistema de leilão simples de primeira ordem, onde os usuários escolhiam quanto estavam dispostos a pagar de taxa por transação (gas fee) para que seus pedidos fossem processados. Os mineradores priorizavam transações de acordo com o valor das taxas, o que gerava: Incerteza de custos e experiência de usuário excessivamente complexa.

A EIP-1559 reformulou esse sistema em quatro principais aspectos:

a. **Base Fee (Taxa Base)**

- *A EIP-1559 introduziu uma taxa base que é ajustada automaticamente pela rede a cada bloco, dependendo do uso da rede. Quando a demanda é alta, a base fee aumenta, e quando a demanda é baixa, a base fee diminui.*

b. Gas Limit **(Limite de Gas)**

- *Com a EIP-1559, cada bloco na rede Ethereum possui um limite de gas duplo, permitindo que o tamanho do bloco varie até o dobro de sua capacidade padrão. Isso permite uma melhor adaptação da rede às flutuações de demanda.*

c. **Priority Fee (Taxa de Prioridade)**

- *Além da base fee, a EIP-1559 introduziu a taxa de prioridade, um valor opcional que os usuários podem adicionar para que os mineradores priorizem suas transações. Essa taxa vai diretamente para o minerador, e não é queimada.*

d. Queima de Ether (ETH Burn)

- *A queima da base fee introduzida pela EIP-1559 retira Ether de circulação permanentemente. Isso ajuda a combater a inflação de emissão de novos ethers pelos mineradores;*

3.5 ETHEREUM 2.0

Nos capítulos acima você deve ter percebido em diversos momentos a menção deste upgrade, nesta seção buscaremos explicar o que ela representa, e os motivos que levaram a sua implementação.

"THE MERGE"

Ethereum 2.0, também conhecido como "The Merge", é uma atualização significativa da blockchain Ethereum que foi projetada para melhorar a **escalabilidade, segurança e sustentabilidade da rede**. As mudanças principais envolvem a **transição** de um sistema de consenso de **proof of work (PoW)**, usado por Ethereum desde seu lançamento, para **proof of stake (PoS)**, e a introdução de uma arquitetura de sharding para fragmentação da rede. A transição aconteceu em setembro de 2022.

RAZÕES PARA A MUDANÇA:

ESCALABILIDADE

A versão original do Ethereum tinha problemas para escalar, especialmente em momentos de alta demanda, o que levava a congestionamentos e taxas de transação muito altas. Com o PoS e o sharding, o Ethereum 2.0 é capaz de processar mais transações por segundo sem sacrificar a segurança ou descentralização, tornando-o mais eficiente e barato para os usuários.

EFICIÊNCIA

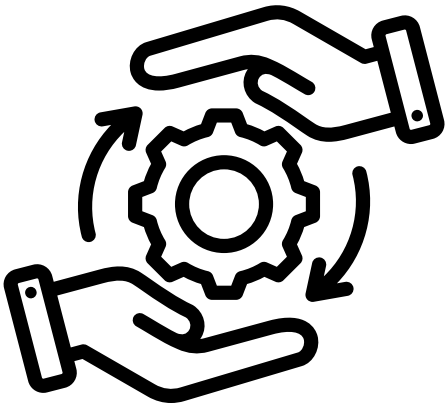
O PoW exige uma quantidade significativa de energia, pois utiliza um grande número de mineradores competindo para resolver problemas matemáticos complexos. O PoS reduz drasticamente o consumo de energia, uma vez que os validadores são escolhidos com base na quantidade de stake que possuem na rede, o que dispensa o uso de processamento intensivo.

SEGURANÇA

Ethereum 2.0 foi projetado para tornar a rede mais resistente a ataques, como o 51% attack, onde um invasor precisaria ter mais da metade do poder de mineração para manipular a rede. No PoS, para comprometer a rede, um invasor precisaria possuir uma grande quantidade de ether (ETH), o que é financeiramente inviável e desincentiva ataques.

PRINCIPAIS MUDANÇAS

- Mudança do **PoW** para o **PoS**
- Sistema de **shards**
  - Mais transações simultaneamente
  - Redução das taxas de execução
- Possibilidade de **novas atualizações**
- Evolução dos **smart-contracts**
  - Smart-contracts mais eficientes e seguros
- Maior **sustentabilidade**
  - Causado pela adoção do PoS



CAPÍTULO 4 - ALTCOINS

Além de Bitcoin e Ethereum, com certeza, muitos já ouviram falar de alguma outra criptomoeda existente, dentre as milhares já criadas. Desta forma, podemos definir o termo **Altcoin,** como sendo qualquer criptomoeda aquém do bitcoin. A combinação entre o sufixo do inglês "alt", significa alternativa e "coin", moeda. Sendo assim, tendo ciência da existência das altcoins, vamos entender mais afundo sobre o assunto, assim como sua importância, surgimento e etc.

O QUE SÃO?

Assim como o Bitcoin, explorado anteriormente, as altcoins consistem em um ativo digital, cujo registro é mantido em um banco de dados, permitindo a negociação das moedas e seu respectivo armazenamento em uma carteira digital, sem que haja a necessidade de uma intermediação de um terceiro, como ocorre com os bancos.

No mercado atualmente, existem, segundo o site CoinMarketCap, 14 mil altcoins, sendo cada uma com um propósito e aplicação específicas. Variam, geralmente, em suas funcionalidades, abrangendo desde entretenimento até soluções voltadas para a privacidade das transações. Uma parte importante é voltada somente para os sistemas complexos de processamento de dados fora da blockchain.

COMO SURGEM AS ALTCOINS?

Agora partindo para seu surgimento e como elas aparecem no "mercado". Em geral, elas são criadas através de um processo técnico, envolvendo a construção da nova criptomoeda a partir de uma blockchain já existente ou pela criação de uma blockchain própria. São formadas, basicamente, por linhas de código, que estabelecem as regras de emissão e circulação de tais ativos.

Em via regra o modo como isso é feito, dependerá dos objetivos primários do projeto e do nível de inovação tecnológica que se pretende alcançar. Em seguida vamos conhecer as principais formas de criação:

FORK - BLOCKCHAIN JÁ EXISTENTE

Um dos métodos mais comuns, o **fork** (bifurcação), em uma blockchain já existente, como Bitcoin. Este método ocorre quando os desenvolvedores copiam o código-fonte de uma criptomoeda e fazem alterações para criar uma nova versão com diferentes regras e funcionalidades

HARD FORK

A nova altcoin é incompatível com a blockchain original, ou seja, após o fork, os nós (computadores que operam a rede) precisam escolher entre continuar com a blockchain original ou passar para a nova.

SOFT FORK

Um soft fork é uma atualização que ainda compatível com a blockchain original, permitindo que alguns nós adotem novas regras enquanto outros, ainda, continuam com as antigas.

ESCOLHA DO ALGORTIMO DE CONSENSO

Um dos principais aspectos ao se criar uma blockchain é: "Como serão validadas as transações? "
Nesse sentido temos o algoritmo de consenso, sendo o Proof of Work (PoW) e o Proof of Stake (PoS) os mais conhecidos além de suas variações.

SMART CONTRACTS

Se a altcoin visa mais do que simples transações financeiras, pode ser necessário implementar um sistema de contratos inteligentes. Eles são basicamente programas de computador que executam automaticamente os termos de um contrato quando certas condições pré-estabelecidas são atendidas.

CRIAÇÃO DE UMA NOVA BLOCKCHAIN

Outra maneira de criar uma altcoins é desenvolvendo uma blockchain totalmente nova e independente. Porém, exige um trabalho mais técnico, envolvendo todo o trabalho de concepção de todo o novo protocoloco da moeda, desde o algoritmo de consenso até as regras para a validação de transações

TOKEN CRIADOS EM PLATAFORMAS EXISTENTES

Em vez de criar uma blockchain do zero, muitas altcoins são criadas na forma de **tokens**, construídos em cima de blockchains já estabelecidas, como a do Ethereum. Esses **tokens** utilizam os padrões técnicos da blockchain hospedeira (como o ERC-20 no Ethereum) para criar novas funcionalidades ou representar ativos digitais.

UTILIZAÇÃO DE SMART CONTRACTS

Os **tokens** são frequentemente criados através de contratos inteligentes, os quais definem as regras de emissão, distribuição e transferência dos tokens. Isso torna o processo de criação muito mais simples do que construir uma blockchain própria.

PROJETOS DEFI E NFT'S

Tokens são amplamente utilizados em projetos de finanças descentralizadas (DeFi) e tokens não fungíveis (NFTs), aproveitando a infraestrutura já existente em blockchains como Ethereum, Binance Smart Chain e Solana.

E as distribuições das novas altcoins?

Após o desenvolvimento das novas altcoins, sua distribuição são realizadas aos usuários, podendo ocorrer de várias maneiras, a depender do seu algoritmo de consenso:

- **Mineração (Proof of Work)**: Mineradores irão competir para validar as transações e assim, receber novas moedas como recompensas;
- **Staking (Proof of Stake):** Validadores recebem recompensas por participarem da rede;
- **ICO (Oferta Inicial de Moeda):** Semelhante ao que acontece no Mercado de Capitais. Equipe vende uma parcela inical para financiar o desenvolvimento do projeto;

QUAL SUA FUNCIONALIDADE?

Independentemente de seu propósito ou funcionalidade, qualquer altcoin pode ser usada para realizar transações e pagar por bens e serviços. O aspecto essencial é que essas movimentações podem ocorrer de forma autônoma, sem depender de um servidor central, de forma que cada um consiga negociar com outra pessoa sem intermediação.

Dessa forma, mesmo que as altcoins sejam vistas como dinheiro virtual, elas representam muito mais do que isso. Vamos conhecer um pouco mais do setor e suas inúmeras funcionalidades possíveis:

1 *Stablecoins*, as moedas pareadas

Stablecoin é um tipo de moeda digital que visa manter paridade com um ativo tradicional, como o dólar e ouro. Embora o termo "stable" signifique "estável", não significa que seu valor seja fixo ou determinado. Mesmo com um depósito de garantia que cobre toda a oferta, as cotações ainda podem apresentar variações. Seu principal benefício é sua menor volatilidade em comparação com outras criptomoedas e uma grande capacidade de realizar transferências sem burocracia. Além disso, cada uma pode adotar um mecanismo próprio para manter sua paridade, podendo incluir titulos de dívida, depósitos bancários, entre outros. Ademais, cada administrador possui diferentes níveis de transparência e garantias sobre suas reservas.

Exemplo 1

Theter USDt (USDT)
- Moeda digital criada em 2014 para espelhar o dólar americano.

PAX Gold (PAXG)
- Moeda digital lastreada em ouro, onde cada token possui 1 onça troy de ouro, ou seja, 31 gramas do ouro.

DeFi, Decentralized Finance 2

As altcoins voltadas para o setor de DeFi (Finanças Descentralizadas) são usadas para criar um ecossistema de serviços financeiros como empréstimos, negociação, seguros e poupança, sem intermediários centralizados, como bancos. Construídas principalmente sobre a blockchain do Ethereum, elas utilizam contratos inteligentes para automatizar e gerenciar transações, garantindo descentralização e maior acessibilidade. As principais aplicações do DeFi incluem empréstimos via contratos inteligentes, exchanges descentralizadas (DEXs) para negociações P2P, derivativos e seguros, além de Yield Farming e Staking para gerar retornos e recompensas.

Exemplo 2

Uniswap (UNI)
- Uma das maiores exchanges descentralizadas (DEXs), permite a votação em mudanças de protocolos e decisões importantes

Aave (AAVE)
- Permite empréstimos e empréstimos colateralizados.

3 *Privacy Coins*, as altocoins de privacidade

Altcoins de privacidade são criptomoedas projetadas para proteger a identidade dos usuários e os detalhes das transações. Elas utilizam tecnologias avançadas, como criptografia, mixagem de moedas e redes anônimas, para garantir que informações como remetentes, destinatários e valores sejam ocultadas ou ofuscadas. O objetivo principal dessas altcoins é proporcionar anonimato, permitindo que os usuários realizem transações sem a preocupação de serem rastreados. Isso é especialmente valorizado em contextos onde a privacidade financeira é crucial, como em transações sensíveis ou em regiões com vigilância intensa.

Exemplo 3

Monero (XMR)
- Foco em extremo anonimato e segurança.

Dash (DASH)
- O PrivateSend mistura as moedas dos usuários em um pool, dificultando o rastreamento de transações. O Dash também oferece transações rápidas e seguras.

Exemplo 4

Litecoins (LTC)
- Versão mais rápida e leve do que o Bitcoin, sendo processados a cada 2,5 minutos (Bitcoin leva 10 min).

Bitcoin Cash (BCH)
- Um fork do Bitcoin com foco em maior escalabilidade, permitindo transações mais rápidas e com menores taxas.

4 *Payment Coins*, Moedas de Pagamento

As moedas de pagamento são altcoins projetadas especificamente para servir como um meio de troca em transações financeiras, funcionando como uma alternativa digital às moedas tradicionais, como o dólar ou o euro. O principal objetivo dessas moedas é facilitar pagamentos rápidos, seguros e de baixo custo, tanto no comércio eletrônico quanto em transferências entre indivíduos. Elas oferecem uma forma descentralizada de realizar transações, sem a necessidade de intermediários, como bancos ou processadores de pagamento, utilizando a tecnologia de blockchain para registrar e validar todas as transações.

5 *Platform Tokens*,os tokens de plataforma

Os tokens de plataforma são criptomoedas nativas de blockchains que permitem o desenvolvimento de aplicativos descentralizados (dApps) e a execução de contratos inteligentes. Esses tokens são usados como combustível dentro dessas plataformas, desempenhando um papel essencial na operação da rede e no suporte à infraestrutura que permite a criação de novos projetos e aplicativos. Eles são mais do que apenas uma forma de pagamento; são fundamentais para a funcionalidade e segurança de suas respectivas blockchains.
Elas são basicamente um combustíevel para a rede (Gas Fees), sendo usados para pagar taxas de transação e execucação dos *smart contracts,* além disso servem de suportes a contratos inteligentes e a desenvolvivemento de dApps.

Exemplo 5

Ethereum (ETH)

Cardano (ADA)
- Oferece contratos inteligentes e soluções mais eficientes, com foco em pesquisa acadêmica e provas científicas.

Solana (SOL)
- Altas velocidades de transações e baixa latência, utilizada para pagar taxas e staking na rede

Exemplo 6

Binance Coin (BNB)
- Inicialmente foi lançado como utility token para pagar taxas de negociação com descontos dentro da exchange Binance.

Chainlink (LINK)
- Utilizado para pagar os operadores de nós (oracles) que conectam contratos inteligentes a dados do mundo real.

6 *Utility Coins*, as moedas de utilidade

As moedas de utilidade (ou utility tokens) são criptomoedas que servem para fornecer acesso a serviços, produtos ou funcionalidades específicas dentro de um determinado ecossistema de blockchain. Diferentemente de outras criptomoedas, como Bitcoin, que são usadas principalmente como reserva de valor ou meio de pagamento, as moedas de utilidade têm um propósito específico relacionado a manter em funcionamento a economia de uma plataforma ou rede, permitindo com que os usuários interajam com o ecossistema e utilizem os serviços oferecidos. Além disso, como forma de incentivo, elas ajudam a promover o crescimento da comunidade de usuários e desenvolvedores, impulsionando a adoção de tecnologias descentralizadas.

7 *Layer 0*

São altcoins projetadas para facilitar a comunicação e o compartilhamento de dados entre diferentes blockchains. Seu principal objetivo é resolver um dos maiores desafios do ecossistema de blockchain: a falta de interoperabilidade entre redes diferentes, como Bitcoin, Ethereum, Solana, entre outras, que normalmente operam de forma isolada. Com elas, é possível transferir ativos, informações e valor entre várias blockchains, criando uma rede de blockchains interconectadas.

Exemplo 7

Polkadot (DOT)
- Plataforma projetada para conectar várias blockchains em um único ecossistema permitindo a transferência de qualquer dado ou ativo.

8 *Meme coins*, criptomoedas-meme

As meme coins são criptomoedas que surgem principalmente como uma piada ou sátira, muitas vezes inspiradas por memes da internet ou eventos culturais populares. Embora comecem como brincadeiras, algumas meme coins ganham uma grande base de usuários e, em certos casos, atingem valores de mercado surpreendentemente altos. No entanto, elas costumam ter pouca ou nenhuma utilidade técnica ou propósito específico além da especulação e do engajamento da comunidade.

Exemplo 8

Dogecoin (DOGE)
- Primeiro meme coin criada em 2013 como paródia do Bitcoin.

Pepe Coin (PEPE)
- Inspirada no famoso meme **Pepe the Frog**.

Altcoins de Gaming 9

As altcoins de gaming são criptomoedas voltadas para o ecossistema de jogos, sendo utilizadas em plataformas de games baseadas em blockchain. Elas servem para impulsionar a economia interna dos jogos, possibilitar a compra de itens digitais, recompensar jogadores por conquistas ou participações e, muitas vezes, permitir a criação de um modelo econômico play-to-earn (jogue para ganhar), onde os jogadores podem ganhar dinheiro real jogando.

Exemplo 9

Axie Infinity (AXS)
- Um dos jogos mais populares, onde os jogadores criam, batalham e negociam criaturas chamadas **Axies.** Os jogadores podem ganhar **Smooth Love Potion (SLP)**.

E OS OUTROS ATIVOS DIGITAIS?

Além das altcoins, existem outros ativos digitais que não são considerados especificamente moedas alternativas, mas fazem parte e tem seu lugar no mundo das criptomoedas. Eles podem incluir diferentes formas de representação de valor, dados, ou direitos sobre algo, mas não são projetados para serem fungíveis ou utilizados como moedas.

1 *NFT's (Non-Fungible Tokens)*

Os NFTs (Non-Fungible Tokens) são tokens digitais exclusivos que utilizam a tecnologia blockchain para representar a propriedade de um ativo específico e não replicável. Ao contrário das criptomoedas como Bitcoin ou Ethereum, que são fungíveis (ou seja, cada unidade é idêntica e intercambiável), os NFTs são não fungíveis, o que significa que cada um deles é único e não pode ser substituído por outro de igual valor.

Exemplo NFT's

Bored Ape Yacht Club (BAYC)
- São 10.000 imagens únicas de macacos desenhados em estilo cartoon, sendo as mais valiosas se tornando um **símbolo de status**.

RWA (Real World Assets) 2

Os RWA (Real World Assets) são ativos do mundo real que foram tokenizados e registrados em uma blockchain, permitindo que esses ativos físicos ou financeiros sejam representados digitalmente. A tokenização de RWA cria novas oportunidades para negociação, gestão e propriedade de ativos tradicionalmente ilíquidos, como imóveis, ações, títulos, commodities, créditos de carbono, e até mesmo obras de arte. Esse processo de tokenização cria um registro imutável e transparente da propriedade, podendo ser fracionada e aumentando sua liquidez.

Exemplo RWA

imóveis
- Propriedades físicas podem ser tokenizadas, permitindo sua compra fracionada de um imóvel. Plataformas como a RealT oferecem a propriedade fracionada de imóveis por meio de tokens.

CAPÍTULO 5 – ETHEREUM KILLERS

Dentro do segmento de Altcoins, temos outro termo muito comum no segmento das criptomoedas, que é o das Ethereum Killers. Como visto anteriormente, a Ethereum é a segunda maior criptomoeda existente, sendo a mais popular utilizada para contratos inteligentes e aplicativos descentralizados (dApps), porém assim como todas plataformas, também apresenta problemas. E desta forma, na tentativa de resolve-los que surgem as Ethereum Killers.

O QUE SÃO?

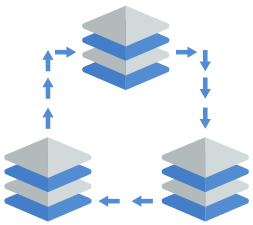
Esse termo diz respeito à um grupo de plataformas da blockchain de layer 1, as quais surgiram como competidoras do Ethereum, oferecendo soluções para os problemas enfrentados pela segunda maior cripto, como escalabilidade limitada, altas taxas de transação (*gas fees*) e velocidades de processamento.

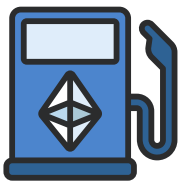
Embora cada uma tenha suas próprias vantagens e desvantagens, todas focam na busca para contribuir para a evolução do ecossistema blockchain, criando soluções mais robustas para o futuro, mais econômicas e eficientes.

QUAIS AS PRINCIPAIS CARACTERÍSTICAS DAS "ETHEREUM KILLERS"?

Escalabilidade

Muitas dessas plataformas utilizam arquiteturas que permitem um maior número de transações por segundo (TPS). Isso é especialmente importante em períodos de alta demanda, quando a rede Ethereum pode sofrer congestionamento.





Taxas de Transação

As "Ethereum killers" geralmente têm taxas de transação mais baixas, tornando-as mais acessíveis para desenvolvedores e usuários, especialmente em aplicações de menor valor.

Contratos Inteligentes

Oferecem suporte a contratos inteligentes, mas frequentemente utilizam linguagens de programação diferentes ou fornecem ferramentas que simplificam o desenvolvimento de dApps.

Interoperabilidade

Algumas dessas plataformas focam em permitir que diferentes blockchains se comuniquem entre si, facilitando a troca de dados e valores entre redes distintas.

Exemplos das "Ethereum Killers"

Como exemplos de Ethereum Killers, podemos citar diversas. As mais famosas são:

- Binance Smart Chain (BSC)
- Cardano (ADA)
- Solana (SOL)
- Polkadot (DOT)
- Avalanche (AVAX)
- Tezos (XTZ)

CAPÍTULO 6 – SOLANA: A MAIOR ETHEREUM KILLER

Solana é frequentemente destacada como uma das maiores concorrentes do Ethereum, principalmente devido às suas características técnicas e capacidades avançadas que abordam algumas das limitações mais significativas enfrentadas pela rede Ethereum. A blockchain de Solana foi projetada com o objetivo de maximizar a escalabilidade, a velocidade de transações e a eficiência de custos, tornando-a uma opção atraente para desenvolvedores e usuários de aplicativos descentralizados (dApps).

O QUE É?

Solana é uma plataforma de blockchain de alta performance que suporta contratos inteligentes e dApps, semelhante ao Ethereum. Fundada por Anatoly Yakovenko em 2017 e lançada inicialmente em 2020, a Solana utiliza uma combinação inovadora de mecanismos de consenso chamados Proof of History (PoH) e Proof of Stake (PoS). Esta abordagem híbrida permite que a Solana alcance altas taxas de transações por segundo (TPS) enquanto mantém os custos de transação baixos.

INOVAÇÃO À BLOCKCHAIN

Proof Of History (PoH)

O PoH consiste em uma função de atraso verificável que registra eventos cronologicamente, ou seja, permite que haja uma verificação na rede, com base no tempo exato que a transação foi realizada, ajudando a reduzir o tempo necessário para alcançar consenso na rede, o que aumenta a velocidade e a eficiência.

+

PoH + PoS

Em conjunto ao PoH, ele utiliza o PoS permitindo que validadores participem da rede com base na quantidade de SOL (a moeda da Solana) que estão dispostos a bloquear como garantia. Isso resulta em um mecanismo de consenso que é energeticamente eficiente e rápido.

SOLANA X ETHEREUM

Em relação ao Ethereum, a Solana é uma alternativa com **maior escalabilidade**, sendo capaz de processar até **65.000 transações por segundo (TPS)**, o que é significativamente superior ao Ethereum, mesmo após sua transição para Ethereum 2.0 e Proof of Stake. Essa capacidade é possível graças ao PoH e à arquitetura de rede otimizada da Solana.

Ademais, devido à sua **alta eficiência**, as taxas de transação na rede Solana são **extremamente baixas**, muitas vezes inferiores a um centavo. Isso contrasta fortemente com o Ethereum, onde as gas fee podem ser bastante elevadas durante os períodos de congestionamento da rede, já que em períodos de baixo congestionamento é de $0,10 (10 vezes maior que a Solana).

Apesas disso, a Solana enfrentou problemas com tempo de inatividade e estabilidade da rede, o que não acontece com a rede Ethereum, por exemplo, que se mostra uma rede completamente consolidada e robusta, sem apresentar instabilidades.

CRÍTICAS À REDE DA SOLANA

Centralização

- **Menor número de validadores**: Com um número limitado de validadores, pode tornar a rede mais suscetível a ataques e falhas, tornando-a mais centralizada e dependente.
- **Requisitos de hardwares elevados**: Os altos requisitos técnicos para rodar um nó na rede podem excluir validadores menores, favorecendo grandes entidades ou empresas, o que contribui ainda mais para centralização.

Downtime e Instabiliade

- **Interrupções de serviço**: A Solana enfrentou várias interrupções significativas, com a rede ficando offline por horas em algumas ocasiões levantando preocupações sobre a confiabilidade da rede.
- **Congestionamento:** Durante picos de atividade, a rede tem mostrado sinais de congestionamento, o que pode afetar o desempenho e a experiência do usuário.

Questões de Segurança

- **Vulnerabilidade e manipulação de mercado:** Assim como qualquer plataforma que suporte contratos inteligentes, pode ser vulnerável a bugs e exploits, levando a perdas financeiras. Além disso, o ecossistema tem sido alvo de bots que podem manipular preços, afetando a justiça nas transações.

COMPARATIVO EM RELAÇÃO A ETHEREUM

Característica	Solana	Ethereum
Ano de Lançamento	2020	2015
Velocidade de Transação (TPS)	29.000 TPS	45 TPS
Taxas de Transação	Menos de $0,01	$1
Mecanismo de Consenso	PoH + PoS	PoS
Ecossistema	Crescendo, com foco em rapidez e baixo custo	Grande, bem estabelecido
Estabilidade	Passou por períodos de inatividade	Geralmente Estável
Centralização	Média/Alta	Baixa

CAPÍTULO 7 - PORQUE INVESTIR NO SETOR

O setor de criptomoedas tem atraído cada vez mais a atenção de investidores, entusiastas da tecnologia e até mesmo de grandes empresas e governos. Já se fala até de proteção de carteira (hedge) ao comprar certos criptoativos. Mas por que esse interesse tão grande? Vamos explorar alguns dos principais motivos:

7.1 INOVAÇÕES

A revolução digital dos últimos anos trouxe consigo uma série de inovações que estão redefinindo setores inteiros da economia. Entre essas tecnologias, blockchain, contratos inteligentes, DeFi e NFTs emergem como as principais forças disruptivas, moldando o futuro da forma como interagimos com dinheiro, propriedade e dados.

BLOCKCHAIN

A base de tudo é o blockchain, uma tecnologia que revoluciona a forma como registramos e verificamos transações. Ao criar um livro-razão digital, descentralizado e imutável, o blockchain garante maior segurança, transparência e elimina a necessidade de intermediários, como bancos. Essa tecnologia, porém, não se limita a transações financeiras.

CONTRATOS INTELIGENTES

Programas autônomos que operam sobre a blockchain, executando automaticamente acordos quando determinadas condições são cumpridas. Imagine contratos de aluguel, seguros ou até mesmo acordos comerciais sendo executados de forma transparente e eficiente, sem a necessidade de intermediários, o que reduz o risco de erros humanos e fraudes.

DE-FI (FINANÇAS DESCENTRALIZADAS)

Conjunto de serviços e produtos financeiros que rodam em uma blockchain. A DeFi democratiza o acesso a serviços financeiros, permitindo que qualquer pessoa, em qualquer lugar do mundo, participe de mercados financeiros sem a necessidade de contas bancárias tradicionais. Isso abre portas para uma nova era de inclusão financeira, com maior acesso a crédito, empréstimos e outros produtos financeiros.

NFTS (TOKENS NÃO FUNGÍVEIS)

Os NFTs representam um marco na digitalização da propriedade. Os NFTs conferem autenticidade e propriedade única a ativos digitais, como obras de arte, itens de jogos e colecionáveis. Essa tecnologia está abrindo novas possibilidades para a criação de mercados digitais e a monetização de conteúdo, transformando a forma como artistas, músicos e criadores de conteúdo interagem com seus fãs.

7.2 EMPRESAS E GOVERNOS

O universo das criptomoedas, antes visto com ceticismo, tem ganhado cada vez mais espaço no cenário econômico global. Grandes empresas, governos e instituições financeiras estão adotando essas moedas digitais, impulsionando uma transformação profunda no sistema financeiro tradicional.

1 Empresas

Gigantes como Tesla e MicroStrategy, por exemplo, realizaram investimentos significativos em bitcoin, demonstrando a crescente confiança no setor e a busca por novas formas de diversificar seus ativos. A adoção corporativa vai além da simples especulação, representando uma estratégia para garantir a competitividade em um mercado cada vez mais digital. o bitcoin ainda é um investimento utilizado por empresas importantes como estratégia de tesouraria.

MicroStrategy:
US$ 14,3 bilhões

Tesla:
US$ 649 milhões

Coin Base:
US$ 567 milhões

Mercado Libre:
US$ 9,45 milhões

2 Governos

Governos ao redor do mundo também estão explorando o potencial das criptomoedas. A China lidera o desenvolvimento de moedas digitais de banco central (CBDCs), com o yuan digital já em fase de testes. El Salvador, por sua vez, foi pioneiro ao adotar o bitcoin como moeda legal, buscando impulsionar a economia e atrair investimentos. Essa movimentação governamental sinaliza uma crescente compreensão do papel que as criptomoedas podem desempenhar na modernização dos sistemas financeiros e na inclusão financeira.

Estados Unidos:
US$ 13,8 bilhões

China:
US$ 13 bilhões

Reino Unido:
US$ 4 bilhões

Alemanha:
US$ 3,3 bilhões

7.3 POTENCIAL DE CRESCIMENTO

O mercado de criptomoedas, ainda em seus primeiros passos, demonstra um potencial de crescimento exponencial. Com a evolução tecnológica, impulsionada por avanços como a Internet das Coisas e a Inteligência Artificial, essa nova classe de ativos tem se expandido para além das transações financeiras, encontrando aplicações inovadoras em diversos setores, como a identidade digital, a votação eletrônica e a otimização de cadeias de suprimentos. À medida que a regulamentação governamental se torna mais clara e a integração com o sistema financeiro tradicional avança, espera-se que o mercado de criptomoedas se consolide como uma classe de ativos relevante e promissora

A aprovação dos ETF´s de Bitcoin e Ethereum:

A aprovação dos ETFs (Fundos de Investimentos) nos Estados Unidos representou um marco histórico para o mercado de criptomoedas. Essa decisão, tomada pela Comissão de Valores Mobiliários dos Estados Unidos (SEC), abriu as portas para que investidores tradicionais e grandes instituições financeiras pudessem acessar o mercado de cripto ativos de forma mais simples e regulamentada.

- **Acessibilidade**
- **Credibilidade**
- **Liquidez**
- **Segurança**

7.3 BTC COMO MOEDA DE RESERVA

1 Escassez

Como já dito, o Bitcoin possui uma oferta ilimitada, que o protege contra a inflação. Por esse motivo muitos acreditam no seu potencial como moeda reserva. o Banco Central Europeu defende a hipótese que "criptoativos podem oferecer uma alternativa especulativa ao financiamento tradicional". O bilionario Mark Cuban inclusive comenta que a vitória do ex-presidente Donald Trump pode significar uma nova era de investimentos no Bitcoin como moeda reserva.

2 Descentralização

Diferentemente das moedas tradicionais, controladas por bancos centrais, o Bitcoin opera em uma rede descentralizada, sem a interferência de governos ou instituições financeiras. Essa característica o torna uma alternativa atraente para aqueles que buscam proteger seus ativos contra a inflação e a instabilidade política.

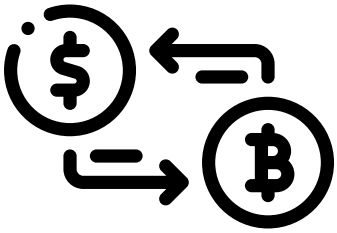
3 Histórico de preços

Ao longo de sua história, o Bitcoin demonstrou um potencial de valorização significativo. Desde sua criação, a criptomoeda experimentou um crescimento exponencial em seu valor de mercado, atraindo a atenção de investidores de todo o mundo.

+ de 4.000.000.000%

2009: 10 US$

2024: 636 Milhões US$



CAPÍTULO 8 - COMO INVESTIR NO SETOR?

Agora que você aprendeu tudo sobre o mundo dos cripto ativos, é hora de colocar em prática e começar a investir seu dinheiro! Mas por onde começar?

8.1 ESCOLHENDO A PLATAFORMA CERTA

As corretoras de criptomoedas são como bancos digitais para ativos digitais. Elas permitem comprar, vender e armazenar suas criptomoedas. Algumas das mais populares são:

Binance
Uma das maiores exchanges do mundo, oferecendo a maior variedade de criptomoedas e ferramentas de negociação.

Coinbase
Uma exchange global com foco em segurança e regulamentação, popular entre iniciantes pela facilidade de acesso.

Mercado Bitcoin
A principal plataforma brasileira, com interface intuitiva e suporte ao real. possui Baixas taxas, Renda fixa digital e conteúdos educacionais.

8.2 Como escolher uma corretora?

A segurança da plataforma é prioridade máxima. Verifique se a corretora possui sistemas de segurança robustos para proteger seus fundos contra hackers e fraudes. Além disso, compare as taxas cobradas nas negociações, depósitos e saques, pois elas podem variar significativamente entre as diferentes plataformas.
Outro ponto importante é a variedade de criptomoedas disponíveis. Escolha uma corretora que ofereça as moedas que você deseja investir, seja Bitcoin, Ethereum ou outras altcoins. Por fim, a interface da plataforma deve ser intuitiva e fácil de navegar, permitindo que você execute suas operações de forma rápida e eficiente.

8.3 ANALISANDO O MERCADO: MÉTRICAS E FERRAMENTAS

Analisar uma criptomoeda exige um olhar atento a diversos fatores. Para tomar decisões de investimento mais assertivas, é fundamental entender as métricas e os indicadores que podem influenciar o desempenho de um ativo digital.

Oferta, Inflação e Demanda

A **oferta** total de uma criptomoeda é crucial: Criptomoedas com oferta limitada tendem a ser mais **valorizadas**, e a **inflação** monetária, ou seja, o aumento dessa oferta total, pode impactar **negativamente** o valor. A **demanda**, por sua vez, é impulsionada por fatores como adoção, desenvolvimento de novos produtos e **especulação**, de maneira que um aumento na demanda geralmente leva à **valorização**.

Capitalização, Volume de Negociação e Volatilidade

A **capitalização** de mercado representa o valor total de todas as moedas em circulação, indicando o tamanho e a relevância de um projeto, enquanto o **volume** de negociação mostra a quantidade de criptomoedas sendo compradas e vendidas, sinalizando o interesse do mercado. A **volatilidade**, ou seja, a variação do preço, é alta em criptomoedas, mas pode representar tanto uma **oportunidade** quanto um **risco**.

OUTRAS CONSIDERAÇÕES:

Tecnologia: A tecnologia subjacente à criptomoeda é fundamental. Avalie a escalabilidade, a segurança e a inovação da rede.
Equipe: A equipe por trás do projeto é outro fator crucial. Uma equipe experiente e com um bom histórico de sucesso aumenta a credibilidade do projeto.
Cases: Entenda os casos de uso da criptomoeda. Quanto mais aplicações práticas ela tiver, maior será a demanda e o potencial de crescimento.
Comunidade: Uma comunidade forte e engajada pode impulsionar o desenvolvimento e a adoção de uma criptomoeda.
Regulamentação: A regulamentação governamental pode ter um impacto significativo no preço e na liquidez de uma criptomoeda.

8.4 SITES PARA CONSULTAR MÉTRICAS

CoinMarketCap: Um dos sites mais populares para acompanhar o preço e a capitalização de mercado das criptomoedas.
TradingView: Uma plataforma de análise técnica que permite criar gráficos personalizados e acompanhar indicadores.
Glassnode: Uma plataforma de análise on-chain que fornece dados sobre a atividade da rede Bitcoin.

Além dessas páginas, existem diversos especialistas no YouTube que podem te ajudar a se manter antenado no mundo dos cripto ativos: **Bruno Perini, Economista Sincero, Investidor 4.20, Paradigma Education, e muitos outros.**