

# Sumário

|   |           |
|---|-----------|
| <b>AULA 1 - Para que serve a filosofia se estamos falando de tecnologia?</b>              | <b>6</b>  |
| O que são crises econômicas?  | 6         |
| 3 crises: 33A.C, 1929, 2007/2008  | 7         |
| Como confiar nas instituições?  | 9         |
| 3 vezes que a soberania das pessoas foi violada.  | 10        |
| SEJA SEU PRÓPRIO BANCO! (Quem quer ser seu próprio banco?)                                | 13        |
| A evolução da internet  | 14        |
| O que é Web 3.0? Existiu uma internet 1.0 e 2.0?  | 16        |
| Quando vamos todos para a Web 3.0?  | 18        |
| HISTÓRICO - Tecnologias que compõe a Blockchain   | 19        |
| CONCLUSÃO, a Ideologia  | 20        |
| <b>AULA 2 - O que é Blockchain e para que pode servir.</b>                                | <b>21</b> |
| Mecanismos de consenso  | 21        |
| Mecanismos de consenso alternativos   | 23        |
| As características da Blockchain  | 24        |
| Potenciais casos de uso   | 27        |
| Futuro da tecnologia  | 29        |
| <b>AULA 3 - Como funciona a Blockchain</b>  |           |
| <b>- A Blockchain é um conjunto de tecnologias de registros imutáveis e distribuídos.</b> | <b>31</b> |
| Como funciona a internet?   | 31        |
| Criptografia  | 34        |
| Como funciona a Blockchain  | 36        |
| Como funciona a mineração do Bitcoin  | 37        |
| <b>AULA 4 Tipos de tokens aula 1: Principais tipos de tokens</b>                          | <b>39</b> |
| Diferença entre moeda e token   | 39        |
| Fungibilidade e não-fungibilidade   | 40        |
| Tokens não fungíveis  | 40        |
| Smart contracts   | 40        |
| Principais tipos tokens/moedas  | 41        |
| Principais projetos   | 42        |
| Principais redes  | 45        |
| Como stablecoins são pareadas (peg)   | 47        |
| Perigos das stable coins - história da luna   | 49        |
| <b>AULA 5 - Tipos de tokens aula 2: NFTs, governança e maluquice</b>                      | <b>51</b> |
| O que é NFT então?  | 51        |
| Colecionáveis não erc-721   | 52        |
| Para que servem e para que não servem os NFTs!  | 53        |
| Soulbound/PFP   | 54        |
| Governança  | 54        |

|   |           |
|---|-----------|
| Representação De ativos da vida real  | 55        |
| <b>AULA 6 - Tudo o que você precisa saber sobre whitepaper</b>  | <b>56</b> |
| O que é um whitepaper?  | 56        |
| Por que é tão importante?   | 57        |
| Como ler um whitepaper resumidamente  | 57        |
| As principais partes do whitepaper  | 58        |
| Como funcionam modelos econômicos   | 59        |
| História do Axie Infinity   | 60        |
| <b>AULA 7 - Tokenização</b>   | <b>62</b> |
| Como funciona e a ideia da tokenização  | 62        |
| Projetos de tokenização fora do comum   | 63        |
| Collateral/Iastro/PEG   | 64        |
| Tipos de NFT (padrões)  | 65        |
| <b>AULA 8 - Negócios Blockchain, além do Bitcoin - P2P(?), exchanges(CEX/DEX), L2, gateways de pagamento e outros</b> | <b>67</b> |
| The Bitcoin Standard  | 68        |
| Exchange, seu banco?  | 70        |
| DEX x CEX   | 70        |
| Marketplaces  | 72        |
| Camada dois (L2, Layer 2)   | 73        |
| Serviços importantes do mercado de criptomoedas   | 75        |
| O que é liquidez e Marketing Maker  | 77        |
| Potencial Business - seguro de vida, auditoria, monetização de games, gestão de operações complexas                   | 77        |
| História do crash da FTX  | 79        |
| <b>AULA 9 BLOCKCHAIN para nerds vol 1</b>   | <b>81</b> |
| Por que Blockchain para nerds?  | 81        |
| O que é o trilema blockchain?   | 81        |
| Análise do trilema em algumas moedas  | 83        |
| Centralizado, descentralizado, distribuído  | 83        |
| Importância da distribuição do poder econômico motivo do bitcoin existir  | 85        |
| Modelo stock-flow   | 86        |
| Ferramentas de análise on-chain   | 87        |
| RPC - Remote Procedure Call   | 89        |
| UTXO - Unspent Transaction Output   | 90        |
| MEMPOOL   | 91        |
| <b>AULA 10 BLOCKCHAIN para nerds vol 2</b>  | <b>91</b> |
| Layers  | 91        |
| ZK - Zero-Knowledge Prove   | 95        |
| O que são Derivativos   | 96        |
| Como funciona day trade   | 97        |
| O que são Bridges   | 97        |
| EVM - Ethereum Virtual Machine  | 98        |

## AULA 11 BLOCKCHAIN para nerds

99

|  |     |
|--|-----|
| Defi, Gamefi, e outras trends                  | 99  |
| Yield hacking                                  | 101 |
| Teoria dos Jogos                               | 102 |
| AirDrop  | 103 |
| O que é ESG                                    | 104 |
| DAOs (Organizações Autônomas Descentralizadas) | 105 |



# PREFÁCIO

Olá jovem pensador.

A jornada que você vai viver conosco não começa nem termina nesta comunidade, páginas, vídeos, certificados e tarefas. Metaforicamente gostamos de dizer que estamos travando uma batalha contra a desinformação a respeito das criptomoedas, Bitcoin e tecnologia blockchain mas, a realidade é que, estamos travando uma guerra contra a falta de consciência a respeito das áreas relacionadas com os seguintes assuntos, ou seja, o Bitcoin ser uma moeda digital, é um fato mas, o debate que ele gera a respeito de valor e a respeito do papel das instituições é o que realmente nos interessa.

O que nos interessa é como essas tecnologias estão mudando nossa percepção sobre o mundo e sobre nós mesmos. Como a tecnologia blockchain está modificando nossas relações e como ela pode gerar valor.

A capacidade de gerar e armazenar valor está diretamente relacionada à necessidade que o ser humano tem de construir um ambiente que o mantenha seguro (ou que ao menos que passe essa sensação).

O governo, a medicina, a polícia, a propriedade privada, os bancos, seguradoras e muitos outros serviços estão diretamente ligados a essa necessidade. Caso você ainda não tenha questionado essas instituições/entidades ou serviços/pactos, nosso objetivo é que, passe a fazê-lo pois o núcleo da tecnologia Blockchain questiona todas as relações de poder da sociedade.

Uma vez que o homem passou a dominar a tecnologia da agricultura, deixou de ser sedentário, sendo o termo usado, no caso, em oposição a nômade, que é o modo de vida do “homem das cavernas”, ou seja, que vive em uma área, esgota os recursos do local e se move para o próximo e assim por diante.

Ou seja, uma vez que o homem foi dominando os conhecimentos sobre

agricultura, criação de gado e de outros animais além da construção de abrigos mais complexos, se tornou necessária também a proteção desse patrimônio. Muitas das instituições mencionadas acima são produtos dessa necessidade, direta ou indiretamente.

A gestão dessas novas relações foi o que motivou a criação de pactos sociais como as relações de trabalho, o dinheiro, o governo e a ideia de \propriedade privada.

**“Tecnologia pode ser definida como a aplicação do conhecimento para atingir objetivos práticos de maneira específica e replicável.”**

O poder da tecnologia é imenso e a crescente adoção/difusão de uma tecnologia gera um crescimento exponencial pois, a partir daquele momento, as pessoas vão construir sob aquele conhecimento, como uma plataforma, e é por isso que tudo que for falado aqui deve ser considerado não como um ponto de chegada mas sim de partida para que possamos nos fazer as perguntas certas e, por tanto, construir, com bases e fundamentos sólidos, o futuro usando a incrível tecnologia que é a blockchain.

# AULA 1 - Para que serve a filosofia se estamos falando de tecnologia?

A internet foi e é uma tecnologia revolucionária. Ela foi plataforma para milhares de revoluções, bem como o desenvolvimento de infinitas novas possibilidades. A internet é vista como um direito humano e oferece acesso e oportunidades nunca antes vistas.

Tudo ocorre através da internet hoje em dia, inclusive coisas que antes eram bastante restritas à atividade presencial, como fazer compras. Seria natural imaginar que, em algum momento, haveria um dinheiro digital, mas por algum motivo foi necessário uma grande crise e um grande aumento da desconfiança nas instituições para isso acontecer.

A realidade é que, desde a década de 80, já existiam pessoas pensando em criar uma espécie de dinheiro digital porém nem a melhor ideia do mundo pode convencer uma pessoa que não percebe sua utilidade e, foi só após o crash de 2007/2008, que a humanidade conseguiu o marco de "conquistar" sua primeira moeda digital (descentralizada): O Bitcoin.

## O que são crises econômicas?

Algumas definições de economia encontradas no google são:

*"Uma economia é um sistema de atividades de produção e consumo que determina como os recursos são alocados entre todos os seus participantes."*

*"A economia é um sistema de distribuição de recursos limitados."*

*"Economia é o sistema de comércio e indústria pelo qual a riqueza de um país é feita e usada"*

*"Uma economia é uma área de produção, distribuição e comércio, bem como consumo de bens e serviços. Em geral, é definido como um domínio social que enfatiza as práticas, discursos e expressões materiais associadas à produção, uso e gestão de recursos escassos'."*

Todas apontam para que a economia é um sistema de criação/distribuição/consumo de recursos/serviços porém conforme nos movemos para algumas áreas os conceitos podem se tornar incrivelmente vagos ou subjetivos, por exemplo:

Quanto vale um pão? Um barril de petróleo? Um diamante? Uma ideia?

O conceito da expressão “de milhões” exprime de maneira bem humorada o quanto relativo pode ser o valor percebido de qualquer coisa. (por exemplo: jantar de milhões, ideia de milhões, rolê de milhões)

As crises são desequilíbrios que podem ser causados por diversos fatores e causam o colapso total ou parcial do sistema.

### 3 crises: 33A.C, 1929, 2007/2008

> Roma Antiga

O governo da época não conseguiu controlar as altas taxas de juros praticadas ilegalmente que, além de tudo, eram praticadas pelos próprios parlamentares. O sistema jurídico sofria com essas demandas e, em uma tentativa de resolverem o problema exigindo que as dívidas fossem parcialmente pagas e que aqueles que emprestam dinheiro tivessem terras em conformidade com as leis da época dentro de um determinado período acabou por instaurar-se uma crise.

Os credores passaram a cobrar o valor total e, mesmo sem a obrigação legal, por obrigação moral, as pessoas se viram forçadas a fazer isso e, por isso, muitas foram forçadas a venderem suas terras, o que causou uma depreciação muito forte no valor.

O imperador da época, Tacitus, resolveu a crise distribuindo uma quantia considerável de dinheiro para que unidades financeiras de sua confiança emprestassem sem juros com o prazo de 3 anos sendo o valor lastreado 50% em terras. Dessa maneira as pessoas não precisavam vender suas terras o que diminuiu a demanda e normalizou a situação.

### > 1929, uma “crise especulativa”

A crise de 1929 é dita como a pior crise de todos os tempos. Ela é atribuída à natureza especulativa dos investimentos na época, além de uma falta de projeção.

Após o fim da primeira guerra, a Europa se erguia lentamente e, por falta de um pátio industrial, afinal de contas havia sido o cenário da guerra, acabava importando quase tudo dos EUA.

Porém a Europa, uma vez mais estruturada, passou a produzir muito do que importava e, mesmo assim, o mercado continuou valorizando até que uma série de vendas em massa causou a maior crise da história.

O índice Dow Jones caiu por 4 anos consecutivos de uma máxima de 384 pontos até um mínima 41 pontos de maneira que o mercado demorou mais de 20 anos para recobrar os mesmos patamares de valores anteriores à crise.

### > 2007/2008, uma crise de confiança.

A crise de 2008 lembra um pouco a de 33 A.C. por envolver o setor de moradia, porém é mais complexa por conta do mundo ser bem também bem mais complexo.

“Empréstimos predatórios direcionados a pessoas de baixa renda que buscavam comprar casas de baixa renda, instituições financeiras globais tomado riscos demasiados e a bolha imobiliária dos Estados Unidos estourar culminaram em uma “tempestade perfeita”.”

É o que diz o wikipedia e, de fato, é um bom resumo. Porém como as instituições que deveriam fiscalizar esses abusos, de certa maneira, ou protagonizaram o escândalo, fizeram vista grossa ou simplesmente não conseguiram impedir a crise e, no momento que realmente a crise se intensificou, o governo prestou socorro, com o dinheiro do contribuinte, aos bancos e instituições que eram as próprias responsáveis pelo incidente.

Por isso a crise de 2007/2008 foi uma crise de confiança. Após essa crise

muitos diriam que somente uma pessoa que desconhece esses fatos (ou uma pessoa maluca) confiaria suas finanças a essas instituições.

**Mas existe uma solução para esse problema?**

### **Como confiar nas instituições?**

A resposta simples é: Não confiando! Nenhuma instituição precisa de confiança de ninguém para ser eficiente, o que elas precisam, além de cumprir seu papel, é da fiscalização das pessoas e, para que isso ocorra, é necessário transparência e auditorias contínuas e, melhor ainda se forem em tempo real.

Não podemos esquecer que, em muitos momentos na história, as instituições e governos falharam não apenas por conta do acontecimento das crises econômicas que mencionamos mas inclusive por roubar o próprio povo, legalizar o racismo (Apartheid), e até promover o extermínio em massa (nazismo). O que deixa claro que não existem limites para a extensão do perigo que as instituições e governos podem oferecer quando mal gerenciados/intencionados.

### **3 vezes que a soberania das pessoas foi violada.**

> Confisco da Poupança em 1990, Plano Collor

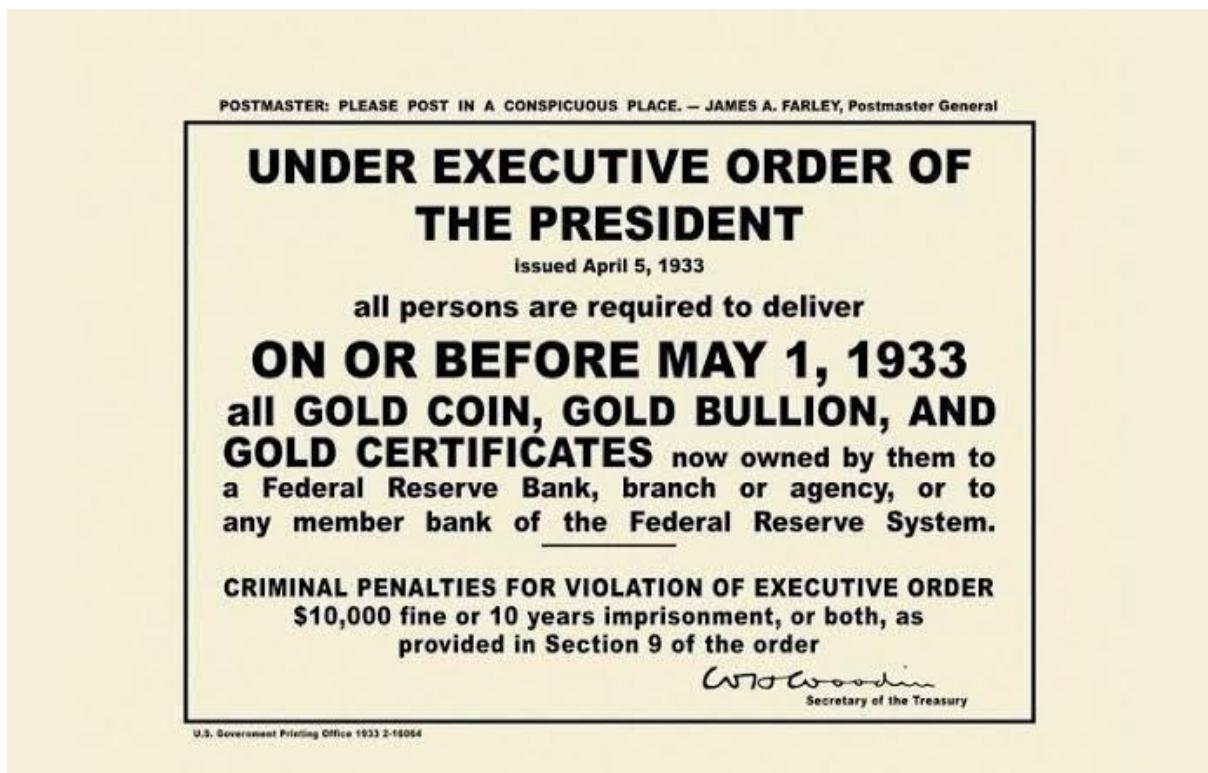


Assumindo o Brasil nas primeiras eleições diretas pluripartidárias, eleito entre nomes famosos, Collor era, teoricamente, uma pessoa simples que não fazia parte dos esquemas de corrupção e poder do país e foi eleito com a promessa de resolver, entre outras coisas, os problemas econômicos que assolavam o país.

Em março ele lançou sua primeira investida que foi chamada de Plano Collor, um conjunto de medidas que visava conter a inflação. Entre as medidas: reter qualquer valor em poupança superior a 50 mil cruzeiros (em torno de R\$5000) por 18 meses. Muitas pessoas alegam nunca terem sido resarcidas.

No ano seguinte, em janeiro de 1991, foi lançado o segundo Plano Collor que também não resolveu muita coisa, o que culminou, no final de 1992, no impeachment de Collor. Sendo apenas em 1994, com o Plano Real, no governo de Fernando Henrique Cardoso, que o governo conseguiu estabilizar a hiperinflação brasileira.

> Confisco do ouro nos EUA



Após a crise financeira de 1929 o governo americano implementou uma série de medidas para tentar conter a crise. Uma delas foi romper com o "Gold Standard" que era um lastro que existia entre todos os dólares circulando e as reservas que o governo possuía.

Além disso, o governo decretou que qualquer cidadão que possuísse uma certa quantia de ouro teria que vender ao governo por valores significativamente menores do que os de mercado.

Apesar de escassos os registros de pessoas que foram perseguidas por não cumprir com a regra, em detrimento da população em geral apoiar as medidas governamentais, as pessoas poderiam ser multadas, presas ou ambos por não cumprirem com as normas e, de fato, algumas foram.

> Os Impérios digitais da informação

Se ninguém paga para usar o Facebook como o Mark Zuckerberg se tornou um dos homens mais ricos do mundo? Vendendo os dados das pessoas! Ele foi, inclusive, investigado juridicamente por congressistas americanos e

dividiu opiniões em seus depoimentos, diferente dos congressistas que deixaram claro para todo mundo que não entendem nada de tecnologia.

Mesmo que não seja ilegal é eticamente questionável enriquecer vendendo os dados de outras pessoas. Por esse motivo existem diversas soluções de privacidade como o Brave Browser (o navegador onde esse livro está sendo escrito, nesse momento) que protegem a privacidade de quem usa ele e, quando vende algum dado para algum anunciantre, recompensa o usuário.

Da mesma maneira existem empresas como a Global Analytica que assumiram publicamente recolher dados em massa e usar para manipular as pessoas o que trouxe a volta de movimentos extremistas em vários países do mundo, inclusive nos Brasil e EUA!

Conforme os algoritmos e inteligências artificiais avançam fica mais difícil das pessoas conseguirem desenvolver a "inteligência real" e senso crítico pois são bombardeadas desde o nascimento por dispositivos de engenharia social altamente aditivos que tornam todo crescimento real, aquele que precisa de esforço e encontra dificuldades, algo extremamente desinteressante.

O que os impérios digitais fazem, muitas vezes, é resolver problemas que não eram problemas, criando problemas reais, diminuindo nosso senso crítico, de propósito e violando nossos direitos individuais como a privacidade para escravizar as pessoas e lucrar nesse processo.

#### > Conclusão, Panamá Papers e WikiLeaks

Nosso objetivo como pensadores é questionar as estruturas de poder e pactos sociais e econômicos para conseguir aplicar a tecnologia blockchain de maneira realmente revolucionária e não apenas replicando aquilo que já foi feito.

A soberania do indivíduo ser respeitada quer dizer, na prática, instituições e governos que cooperam para garantir que as pessoas tenham seus direitos respeitados e não os usem para os propósitos que servem aos interesses das pessoas que compõem essas entidades.

A palavra “conclusão” pode levar a ideia de que acaba aqui o assunto, porém, é apenas um começo. Existem muitos governos, entidades e pessoas corruptas fazendo coisas inimagináveis mundo afora. Não cabe a nós, nesse curso, abordar todas essas atitudes e injustiças aqui, mas gostaríamos de convidar você para que o fizesse.

O site WikiLeaks ajuda a disseminar informações confidenciais para o público. Um dos documentos que ajudou a divulgar foi o Panama Papers que trazia o registro de contas Off-shore de muitas pessoas públicas que usavam o sistema para lavar dinheiro e não pagar impostos.

Alguns dos nomes incluem Vladimir Putin, presidente da Rússia, o presidente chinês, Xi Jinping, Nawaz Sharif, ex-primeiro-ministro do Paquistão e até o craque do futebol Lionel Messi.

## **SEJA SEU PRÓPRIO BANCO! (Quem quer ser seu próprio banco?)**

A crise atingiu seu clímax em meados de setembro de 2008 com a falência de um banco americano tradicional (Lehman Brothers). 6 semanas depois, no dia 31 de outubro, um usuário com o nick de Satoshi Nakamoto enviou um e-mail, para uma lista seleta de destinatários de um grupo cypherpunk, contendo o whitepaper do Bitcoin.

Alguma discussão se sucedeu e, no ano seguinte, em 2009, algumas pessoas começaram participar da rede do Bitcoin que é uma moeda digital como nenhuma outra.

O lema do Bitcoin é “Seja seu próprio banco” em partes por conta da crise, porém, inclusive, por conta de um pensamento preexistente da ideia de se libertar das instituições de controle incluindo governos e bancos centrais.

A esmagadora maioria das pessoas se relacionam com as criptomoedas buscando ganhar dinheiro, em segundo lugar temos os apaixonados por tecnologia, mas o grupo que mais cresce é o daqueles que fazem negócios dentro dos parâmetros da blockchain, a tecnologia do Bitcoin. Porém o que começou tudo foi a busca por um ideal de liberdade alimentado pela

incompetência das instituições de provarem equivocadas as preocupações dessas pessoas mais preocupadas com os perigos que o benefício de ceder o controle às instituições.

O Bitcoin é um dinheiro controlado pelo código, livre de erros humanos. O poder atrelado à emissão e gestão de dinheiro é delegada aos usuários que permitem que a rede funcione em seus computadores e não precisa de nenhuma entidade adicional. É 24 horas por dia, transparente, rastreável, não possui CEO nem sede corporativa, porém também não tem atendimento ao cliente e, por um erro bobo você pode perder todo seu dinheiro. Achou que ser seu próprio banco seria fácil?

A maioria das pessoas não querem ter seu próprio banco e arcar com todas as consequências (boas e ruins) que advém. A maioria quer apenas o lado bom, ou seja, ver seu patrimônio multiplicar 10,20,30 vezes no mercado, porém acabam suscetíveis a golpes e a "precisar" confiar em outras instituições, os novos bancos, as exchanges (Corretoras). O que nos faz questionar, "no fim do dia", se as pessoas querem mesmo ser seus próprios bancos.

## A evolução da internet

A maior parte das pessoas vivem imersas na internet. Ela é presente em todos os aspectos do nosso dia-a-dia mas, mesmo assim, o entendimento sobre ela, muitas vezes, é bastante subjetivo. Quer ver?

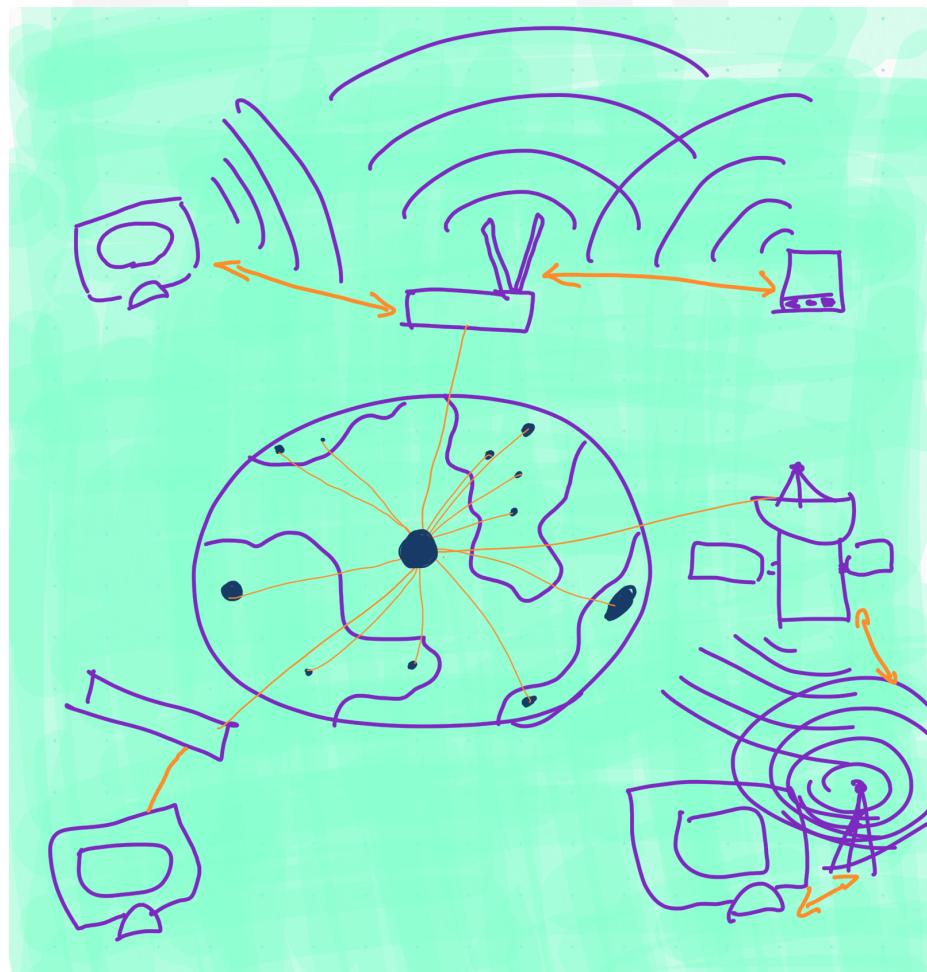
Vamos fazer um exercício, escreva abaixo, em suas palavras, de maneira simples, o que é internet:

Não existe apenas uma definição correta mas, para nossa compreensão escolhemos a seguinte definição de internet:

A internet é uma rede de computadores que se comunica através de protocolos padronizados possibilitando que pessoas acessem arquivos em computadores do mundo todo.

A imagem abaixo retrata de maneira simplificada como funciona a internet. Possuímos dispositivos como computadores e celulares que se conectam através de cabos, modems e antenas a provedores de internet que conectam suas máquinas a estrutura da internet representada pelos pontos azuis.

Essa estrutura possui um problema, entretanto... observe a imagem e tente descobrir como alguém poderia acabar com a internet.



Todas as conexões convergem para um único ponto, ou seja, caso este ponto seja destruído os outros participantes não podem mais se comunicar.

Como podemos resolver isso? Escreva suas ideias abaixo!

Não precisa se preocupar se sua resposta soar maluca ou não solucionar o problema, o importante é o exercício criativo e, além disso, esse problema já possui solução e vamos falar a respeito disso a seguir.

## O que é Web 3.0? Existiu uma internet 1.0 e 2.0?

Talvez seja a primeira vez que você se depara com o termo web 3.0, talvez não e, provavelmente, em ambos os casos, você deve estar se perguntando “e existiu uma internet 1.0 e 2.0?”. E a resposta é: sim!

Inicialmente a internet era uma tecnologia militar destinada a trocar dados sensíveis porém, uma vez que foi criado um protocolo de comunicação universal e ele foi decretado como padrão militar, não demorou muito tempo para empresas como a IBM adotarem o padrão e passarem a oferecer computadores e acesso à internet para o cidadão comum.

O apelo era direcionado principalmente ao acesso a informações de maneira instantânea e realmente se tornou uma ferramenta indispensável para cientistas e estudiosos. (Web 1.0)

Mesmo assim, foi apenas com o Boom das mídias sociais como Youtube, Instagram e outros que a adoção da internet saltou para até 90% em algumas regiões do planeta. (Web 2.0)

A internet é uma das tecnologias mais antigas e é, provavelmente, a mais importante para o funcionamento das criptomoedas. Existem maneiras criadas para que, mesmo sem internet, seja possível realizar transações com Bitcoin, porém, dentro das condições normais, a tecnologia que permite a existência das criptomoedas, a blockchain, usa a internet para criar uma rede menor que funciona dentro de determinados critérios compartilhando recursos e o fruto do trabalho conjunto. (Web 3.0)

Ou seja, inicialmente a internet era para trocar informações estáticas e só passou a ser relevante quando as pessoas passaram a contribuir com a criação do conteúdo e, com a tecnologia Blockchain, passou a permitir que pessoas do mundo todo compartilhassem recursos e os resultados dos seus esforços.

Um exemplo de web 3.0 é a rede do Bitcoin onde todos os participantes cooperam para escrever as transações e criar uma rede segura e, eventualmente, são recompensados em novas moedas criadas pelo código.

#### > WEB 1.0:

Ela foi marcada pelo início da internet e compartilhamento de informações bem como esses sites incríveis que você pode ver nas imagens abaixo.

#### > WEB 2.0:

O termo foi criado em 1999 porém popularizado apenas no ano de 2004 com a primeira conferência que possuía o termo no próprio título (Web 2.0 Conference).

É “a internet” que onde estamos mais presentes através de aplicativos como whatsapp, youtube, instagram, facebook, tik tok e outros. Aqui a identidade passa a ser portatil e podemos logar em muitos lugares com nossas credenciais de gmail, facebook e algumas outras.

#### > WEB 3.0:

O termo foi criado para designar a internet do valor, do compartilhamento de recursos, da cooperação. Representa também, na grande maioria dos casos,

uma mudança radical de pensamento. Enquanto a web 2.0 deu ferramentas para as pessoas fazerem aquilo que já fariam instintivamente, se comunicar, a web 3.0 é uma plataforma para criação de modelos de negócio, cooperação e transparência sem precedentes.

O que faz a web 3.0 tão valiosa são os fundamentos sob os quais foi desenvolvida. O Bitcoin pode até ter um preço e ele oscila, com certeza, porém, o valor da tecnologia blockchain, criada para que ele pudesse vir a existir, rompe com diversos paradigmas. Por exemplo: necessidade de uma entidade, instituição ou governo para controlar o dinheiro. Agora o código faz isso, de maneira 100% resistente à falha humana. Além disso, instituições como os bancos e até advogados são potencialmente descartáveis pois ninguém precisa “confiar” em ninguém, novamente, o código faz a mediação das relações.

Tudo isso é possível por conta da tecnologia blockchain oferecer confiança através da criação de um sistema seguro e criação de registros imutáveis. Parece relativamente simples, mas as implicações são profundas e já estão modificando profundamente nossa maneira de fazer negócios e nos relacionar.

## **Quando vamos todos para a Web 3.0?**

A verdade é que nunca vamos “nos mudar” para nenhuma internet. Essa separação é apenas uma questão de classificação e entendimento humano que, de certa maneira, aprecia bastante esse tipo de organização. Talvez não existe uma internet 1,2 e 3 e seja tudo uma invenção do ser humano, bem como a internet, né? Rs

E, indiferente das provocações filosóficas acima, vamos sempre estar alternando entre os estados de leitores/escritores, criadores de conteúdo/audiência e criadores/tomadores de valor.

## **HISTÓRICO - Tecnologias que compõe a Blockchain**

1973 - Robert Kahn e Vinton Cerf começam a trabalhar juntos no que se tornou o protocolo unificado de comunicação da internet, o protocolo TCP/IP. Em 1974 a primeira versão dele foi para o ar e após vários experimentos o departamento militar decretou o protocolo como padrão para redes militares em 1982 e, posteriormente, ele foi adotado por empresas como a IBM como sendo o padrão comercial em 1985.

Nesse meio tempo, em 1979, Merkle descreveu uma abordagem para distribuição de chaves públicas e assinaturas digitais chamada "autenticação de árvore" (tree authentication), em sua tese de doutorado para a Universidade de Stanford.

1982 - David Chaum descreve uma metodologia de segurança para estabelecer, manter e criar confiança dentro de sistemas de computadores em dissertação para a Universidade Berkeley. Essa ideia já incorporava muitos dos conceitos atuais de blockchain.

1989 - Chaum inventa o dinheiro digital e fundou a corporação DigiCash.

1991 - Stuart Haber e Scott Stornetta, preocupados com a integridade dos dados, criaram uma solução que transforma documentos em um código único (hash) e os agrupa sequencialmente e os temporiza formando uma cadeia.

1992 - Haber e Stornetta acrescentam a árvore Merkle que permite que múltiplos documentos sejam parte de um único registro.

1994 - Haber e Stornetta abrem sua própria Start Up "Surety Technology" mas não conseguem vender sua ideia e acabam sem muito sucesso em suas operações.

1997 - Adam Back cria hashcash, um algoritmo de prova de trabalho (PoW) que seria implementado para impedir ataques cibernéticos através da

verificação do esforço computacional usado para limitar os e-mails com spam.

1999/2002 - O nascimento e morte do Napster, mesmo com seu servidor centralizado, popularizou a tecnologia de conexão direta entre usuários P2P (Peer-to-peer, ponto-a-ponto)

2004 - Hal Finney (Harold Thomas Finney II), famoso cientista da computação e ativista cripto, que viria a ser a primeira pessoa a receber uma transação de Bitcoin, introduziu um sistema chamado RPoW, Reusable Proof Of Work. O sistema resolveu o problema do gasto duplo mantendo os dados amplamente disponíveis e auditáveis em tempo real que mais tarde seria adaptado para criar o sistema de prova de trabalho (PoW) usado no Bitcoin.

## **CONCLUSÃO, a Ideologia**

Sabendo dos fatos históricos fica claro que muitas pessoas que contribuíram para a construção da tecnologia blockchain morreram sem imaginar como ela viria a ser e, além disso, muitas dessas pessoas sequer obtiveram real lucro com suas atividades sejam elas acadêmicas ou até comerciais como no caso da Surety Technologies de Haber e Stornetta.

A construção da revolução se deu por motivos ideológicos muito mais que intelectuais ou comerciais. Alguns fragmentos da tecnologia Blockchain foram, de fato, criados de maneira teórica para resolver um problema hipotético em uma época em que nem havia a difusão da internet ou alguma percepção do seu possível valor.

Muito do que estamos construindo com as criptomoedas ainda não tem uma utilidade prática no dia-a-dia e, o que pode parecer não ter muito sentido pode ser alguma ideia revolucionária que ainda necessita de um pouco mais de entendimento das pessoas para ser aplicada. Se diz investir nessas ideias, porém, ao longo dessas páginas e vídeos você vai aprender outras maneiras de ganhar dinheiro com a revolução da web 3.0 seja trabalhando em empresas do ramo, criando soluções ou solucionando outros tipos de problemas da indústria blockchain.

# AULA 2 - O que é Blockchain e para que pode servir.

Blockchain é um conjunto de tecnologias de registro distribuído imutável, ou seja, serve para criar confiança. Muitos computadores participam, criando um ambiente seguro dentro da internet, para criarem registros imutáveis que são interligados sequencialmente (em uma “cadeia de blocos”). Eles podem ser públicos, privados ou híbridos.

O papel das instituições bancárias, por exemplo, é criar um ambiente seguro para que as pessoas possam armazenar e transacionar valores. Porém é natural que, uma vez que a instituição, seja ela qual for, tenha as atividades pautadas em decisões humanas, sempre haverão consequências relacionadas à falha natureza humana e, por mais que alguns erros possam até ser honestos, o preço pode ser muito alto.

É natural que a tecnologia blockchain seja cada vez mais implementada para substituir as instituições. Dessa maneira quem vai gerenciar as relações será o código prevenindo as falhas humanas enquanto cria um sistema transparente e seguro. Por esse motivo estamos diante de uma revolução que pode ser tão significante quanto o advento da internet em si.

## Mecanismos de consenso

São regras/critérios que devem ser seguidos para que se possa escrever novos blocos de informação. Através de um processo que se chama “mineração” onde os participantes da rede verificam e gravam novos blocos de informação.

Cada rede pode ter seu próprio mecanismo de consenso, porém existem dois principais: Proof-of-Work (prova de trabalho) e Proof-of-Stake (prova de participação).

O objetivo de ambos mecanismos é escrever as transações porém eles funcionam de maneiras inteiramente diferentes. Projetos diferentes podem ter alguns detalhes específicos mas, a grosso modo, enquanto no modelo Proof-of-Work (PoW) os usuários usam seu poder computacional para manter

a segurança da rede resolvendo problemas matemáticos, no modelo Proof-of-Stake (PoS) os investidores que possuem mais capital investindo vão sendo elencados para gravar/verificar as transações. Em ambos os casos as transações são validadas por outros usuários e quem escreveu o bloco é recompensado com a moeda nativa.

#### > O Proof-of-Work do Bitcoin

No Bitcoin, para validar uma transação, os mineradores competem para descobrir quem consegue gerar uma espécie de ou "código de barras" muito especial que identifica exclusivamente todas as transações do período.

Esse código identificador chama hash e, para produzir uma hash, o validador combina todos os dados do bloco com um número aleatório até que o resultado final respeite critérios fixados pela rede. No caso da do Bitcoin, a quantidade de 0 com que o código começa.

Depois que um minerador valida com sucesso uma transação e a adiciona a um novo bloco de transações, ele pode transmitir o bloco para o restante da rede Bitcoin. Outros mineradores e nós na rede verificarão o bloco para garantir que ele seja válido e esteja em conformidade com as regras do protocolo Bitcoin. Se o bloco for aceito pela rede, ele é adicionado ao blockchain e se torna uma parte permanente da blockchain do Bitcoin.

O nome “prova de trabalho” se dá por conta do grande esforço computacional envolvido na quantidade de tentativas e cálculos matemáticos necessários para se encontrar uma hash.

#### > O Proof-of-Stake do Ethereum

No algoritmo de consenso Proof of Stake (PoS) do Ethereum os validadores desempenham um papel crucial na garantia da integridade e segurança da rede, verificando se cada transação é válida e segue as regras da rede. Para se tornar um validador na rede, um indivíduo ou organização deve possuir pelo menos 32 ethers alocados/bloqueados na rede.

Com base na quantidade de tokens empregados os valores são selecionados, quanto mais tokens um validador possui alocados, maior é a

chance de ser selecionado para validar transações e ganhar ETH como recompensa. O que acaba centralizando a rede uma vez que aqueles que possuem mais tokens têm maiores chances de serem recompensados.

O Ethereum só se tornou 100% PoS em 2022 e, apesar do modelo ser muito mais eficiente em termos de gasto de energia elétrica, o “the merge” transformou milhões de dólares em máquinas dos mineradores em sucata. Essas pessoas não viram alternativa se não vender os componentes por quilograma sendo que investiram para dar poder a rede e, por tanto, investiram para fazer o Ethereum ser o que é.

O nome “prova de participação” se deve ao fato que o validador prova seu comprometimento empregando seus recursos na rede o que define, também, quanto ativamente ele participa no processo de validação.

## Mecanismos de consenso alternativos

### > Delegated Proof of Stake (DPoS)

Muito parecido com PoS porém permite que o investidor delegue seu poder de voto para outro usuário no processo de tomada de decisão de maneira a favorecer a escalabilidade e eficiência da rede.

### > Proof of Authority (PoA)

Muito útil para Blockchains privados e permissionados. Critérios são definidos por uma entidade central que, baseada em reputação e confiabilidade, seleciona nós para validarem as transações.

### > Proof of Elapsed Time (PoET)

Em sistemas permissionados, onde já existe confiança, os validadores são escolhidos com base no tempo que estão inativos, ou seja, basicamente “o último da fila” é escolhido.

### > Conclusão

Dependendo do propósito, tamanho da operação e quantidade de recursos um ou outro mecanismo pode ser melhor. O mais importante é analisar todos de maneira crítica e entender suas características e em quais situações elas atuam como defeitos ou qualidades.

A escolha de mecanismo de consenso deve ser mais que uma escolha romântica ou baseada em economia de recursos, ela deve ser uma decisão de negócios que seja coerente com os valores e objetivos do projeto.

**O objetivo é estabelecer confiança criando registros criptografados e distribuídos que são assegurados e escritos de maneira descentralizada e auditável respeitando mecanismos/algoritmos de consenso.**

## **As características da Blockchain**

### **> Programável**

A tecnologia Blockchain é programável de várias maneiras. A maneira mais conhecida é através do uso de contratos inteligentes (smart contracts), aplicações auto executáveis com termos escritos em código que são executados assim que certas condições são preenchidas.

Outra forma é por meio de aplicativos descentralizados, ou DApps, que são construídos sobre uma plataforma blockchain e usam sua infraestrutura para operar.

Apesar de plataformas como Ethereum terem mais funcionalidades, a blockchain do Bitcoin também pode ser programada usando ferramentas como script bitcoin para construir aplicações simples como carteiras multi-assinatura ou serviços de custódia.

### > Descentralizada/Distribuída

As Blockchains podem funcionar sem serem controladas por entidades ou organizações. A maneira como cria confiança é usando uma rede de computadores para validar e registrar transações, eliminando a necessidade de intermediários.

A descentralização cria maior segurança e transparência tanto de maneira técnica como institucional, pois esse atributo é mais que um modelo tecnológico, ele é também um modelo de organização que distribui o poder, por exemplo, de criar e controlar dinheiro.

Como não há um ponto central de controle, é muito mais difícil para os hackers atacarem a rede ou para atividades fraudulentas passarem despercebidas. Além disso, todas as transações podem ser registradas em um registro público, como no caso do Bitcoin.

Uma outra característica inerente a redes muito descentralizadas é a baixa performance quando comparadas a redes centralizadas.

### > Segura

A tecnologia Blockchain é segura devido ao uso de criptografia. Criptografia é uma prática de comunicação segura, que envolve o uso de algoritmos matemáticos complexos para codificar e decodificar mensagens. No contexto da blockchain, a criptografia é usada para proteger os dados armazenados na rede, bem como verificar a autenticidade das transações.

### > Imutável

A imutabilidade da tecnologia blockchain refere-se à incapacidade de alterar ou excluir dados que foram registrados anteriormente. Ela é obtida por meio do uso das “hash”, códigos identificadores únicos, como uma especial de “digital” que muda completamente com a alteração de, sequer, uma vírgula.

Essa característica pode ter um impacto muito negativo no caso de ocorrerem erros ou enganos, pois não há como voltar atrás e corrigi-los. Por

esse motivo que, inclusive, os mecanismos de consenso são tão importantes.

#### > Anônima

As transações em um blockchain são registradas usando um endereço único, que não revela nenhuma informação pessoal sobre o usuário. Isso permite que os usuários façam transações sem revelar sua identidade. No entanto, é importante observar que, uma vez que a esse endereço (chave pública) de um usuário é descoberta, todo o seu histórico de transações na blockchain pode ser rastreado, pois os registros em uma blockchain são imutáveis.

Existem três tipos principais de blockchain: público (não permissionada/permissionless), privado (permissionada/permissioned) e híbridas. Blockchains públicas, como a do Bitcoin e do Ethereum, são abertas para que qualquer pessoa participe delas ou audite seus dados. As blockchains privadas, por outro lado, são restritas a um grupo específico de usuários e requerem permissão para ingressar. Os blockchains híbridos combinam elementos de blockchains públicos e privados e podem ser adaptados para necessidades específicas permitindo que algumas informações sejam públicas enquanto omite outras.

#### > Unâime

Para que uma nova transação possa ser registrada, todos os participantes da rede devem concordar com a validade dela. Isso garante a integridade e a segurança da Blockchain, pois qualquer tentativa de manipulação ou alteração dos dados da transação será rapidamente detectada, rejeitada pela rede e o participante punido.

Uma maneira de alcançar unanimidade é por meio do uso de prova de trabalho (POW). Outra maneira de atingir unanimidade é por meio do uso de mecanismos alternativos de consenso, como Proof-of-Stake (PoS) ou Delegated Proof-of-Stake (DPoS). Nesses sistemas, o papel dos mineradores é substituído por validadores que alocam recursos na rede para poderem validar as transações. Isso ajuda a garantir que todos os participantes tenham interesse em manter a integridade da rede e evita qualquer tentativa de fraude ou manipulação.

#### > Temporizada (timestamp)

Os registros contam com data e hora tanto para a criação do código único identificador (hash) quanto para ajudar a garantir que as transações sejam processadas de maneira justa e transparente, pois não podem ser alteradas ou manipuladas depois de registradas na blockchain. No geral, a característica da temporização de data/hora da tecnologia blockchain desempenha um papel crítico no estabelecimento de confiança no sistema.

### Potenciais casos de uso

- > **Criptomoedas:** Bitcoin, Ethereum e outras criptomoedas são o caso de uso real mais conhecido por permitirem transacionar e armazenar valores sem intermediários.
- > **Gerenciamento da cadeia de suprimentos:** rastreio de mercadorias do produtor ao consumidor com custos menores, maior controle na gestão e maior eficiência.
- > **Gerenciamento de identidade e acesso:** armazenamento e verificação segura de informações de identidade.
- > **Sistemas de votação:** sistemas de votação seguros e transparentes que não podem ser hackeados ou manipulados.
- > **Imobiliário:** Rastreamento de propriedades e auxílio na redução de fraudes.
- > **Sistema de saúde:** armazenamento e compartilhamento seguro de registros médicos e aumento de eficiência na gestão.
- > **Educação:** verificando e armazenando credenciais e registros acadêmicos.
- > **Governo:** simplificar os serviços públicos e reduzir a corrupção.

- > **Organizações de caridade e sem fins lucrativos:** garante transparência e responsabilidade em doações e distribuição de fundos.
- > **Energia:** Gestão e comercialização de créditos de energia renovável.
- > **Agricultura:** rastreando a segurança alimentar, gerenciando processos e recursos.
- > **Varejo:** Melhorando a eficiência da cadeia de suprimentos e reduzindo fraudes.
- > **Arte e colecionáveis:** garantindo autenticidade e propriedade.
- > **Música e mídia:** proteção de direitos autorais e distribuição de royalties de maneira automática.
- > **Seguros:** agilizando o processo de sinistros e reduzindo fraudes.
- > **Bancos:** melhorando a inclusão financeira e reduzindo os custos de transação.
- > **Aluguel:** simplificando o processo de aluguel e reduzindo fraudes.
- > **Viagens e turismo:** melhorando a eficiência da cadeia de suprimentos, segurança, transparência e reduzindo fraudes.
- > **Recrutamento:** verificando e armazenando credenciais de emprego de maneira segura.
- > **Recursos humanos:** gerenciamento de registros e benefícios de funcionários.
- > **Negociação de ações:** melhorando a eficiência, diminuindo custos e reduzindo o risco de fraude
- > **Financiamento da cadeia de suprimentos:** melhorando o acesso ao crédito para pequenas e médias empresas.
- > **Esportes:** verificando e rastreando recordes e estatísticas.

- > **Jurídico:** Melhorando a eficiência dos processos jurídicos e reduzindo o risco de fraude.
- > **Internet das coisas (IoT):** permitindo comunicação segura e troca de dados entre dispositivos.

O preço do Bitcoin pode oscilar ou até ir a zero, porém, seu valor como prova de conceito não é tangível, ou seja, seu real valor para a história da humanidade é possível de ser medido.

A tecnologia ainda está nos seus estágios iniciais de adoção e é inegável que já existem muitas aplicações e que, mesmo assim, muitas outras ainda estão por ser descobertas.

## Futuro da tecnologia

A tecnologia Blockchain tem o potencial de revolucionar uma ampla gama de indústrias e mudar a maneira como vivemos nossas vidas. Uma das principais áreas em que provavelmente terá um impacto significativo é no setor financeiro, onde tem o potencial de simplificar e proteger as transações financeiras além de distribuir o poder relacionado à criação e controle de valores.

Outros usos potenciais incluem o gerenciamento da cadeia de suprimentos, onde pode ajudar a aumentar a transparência e a eficiência. No setor de saúde pode ser usado para armazenar e gerenciar registros de pacientes com segurança, além de poder gerenciar recursos e inventários para maior transparência e segurança.

No campo do gerenciamento de identidade, sistemas baseados em blockchain, podem criar registros de identidade seguros e imutáveis, que podem ser usados para verificar a identidade de indivíduos em diversos contextos. Isso pode ter uma variedade de aplicações, inclusive no processo de votação, onde pode ajudar a garantir a integridade das eleições, e no

mercado de aluguel, onde pode ajudar a verificar a identidade de inquilinos e proprietários.

A Internet das Coisas (IoT) é outra área em que a tecnologia blockchain provavelmente terá um grande impacto. Ao usar sistemas baseados em blockchain, é possível criar redes seguras e descentralizadas de dispositivos conectados que podem se comunicar e compartilhar dados entre si. Isso pode ter uma variedade de aplicações, inclusive no setor de energia, onde pode ajudar a otimizar a distribuição de energia, e no setor de transporte, onde pode ser usado para melhorar a eficiência e a segurança dos veículos autônomos.

Finalmente, a tecnologia blockchain tem potencial para ser usada em uma ampla gama de outras indústrias e aplicações. Por exemplo, pode ser usada para criar sistemas de votação seguros e transparentes, para gerenciar e rastrear a proveniência de bens de luxo ou para criar mercados descentralizados para compra e venda de bens e serviços. As possibilidades futuras para a expansão e uso da tecnologia blockchain são realmente infinitas, e estamos apenas começando a arranhar a superfície do que é possível.

# AULA 3 - Como funciona a Blockchain

- A Blockchain é um conjunto de tecnologias de registros imutáveis e distribuídos.

- A confiança é uma necessidade básica do ser humano, essa é a razão que faz a Blockchain ter tanto valor e impacto real no nosso dia-a-dia.

- Passamos de um modelo probabilístico para um determinístico ao mudarmos de um modelo regido pela confiança em constituições, para um onde o código faz a mediação de nossas relações.

- A web 3.0 capacita a cooperação sem precedentes onde as pessoas compartilham recursos e o resultado dos seus trabalhos globalmente de maneira segura (idealmente, 100% regida pelo código, smart contracts, etc).

- Estima-se que a cultura resultante pode ser de valorizar a privacidade mas também de maior transparência. À medida que nossas informações importantes forem adicionadas aos registros permanentes em blockchains, mentir/omitir vai se tornar, progressivamente, mais antiquado e difícil.

## Como funciona a internet?

A compreensão da internet ter várias camadas. Existem aqueles que são usuários e precisam saber a url dos sites que acessam, existem aqueles que estudam na internet ou produzem conteúdo e precisam de maior domínio das ferramentas e também existem os especialistas/desenvolvedores e, além deles, aqueles que são evangelistas.

O termo “evangelista” surgiu no começo da internet para descrever especialistas que não impulsionaram a adoção da tecnologia, ou seja, que se preocupavam em como comunicar as utilidades ao público e, inclusive, em como ampliar o leque de utilidades para servir as pessoas.

> Características da internet

> **Descentralizada:** A internet não possui um único ponto de controle. Ela é composta de muitas redes interconectadas administradas por diferentes organizações e indivíduos.

> **Comunicação ponto a ponto:** Os dispositivos na Internet podem se comunicar diretamente entre si sem a necessidade de uma autoridade central.

> **Escalabilidade:** A internet pode acomodar facilmente um grande número de dispositivos e usuários, pois novos pontos de operação(nós) podem ser adicionados à rede com facilidade.

> **Padrões Abertos:** A internet é baseada em padrões abertos (open source), como o Transmission Control Protocol/Internet Protocol (TCP/IP), que permitem a interoperabilidade entre diferentes sistemas e tecnologias.

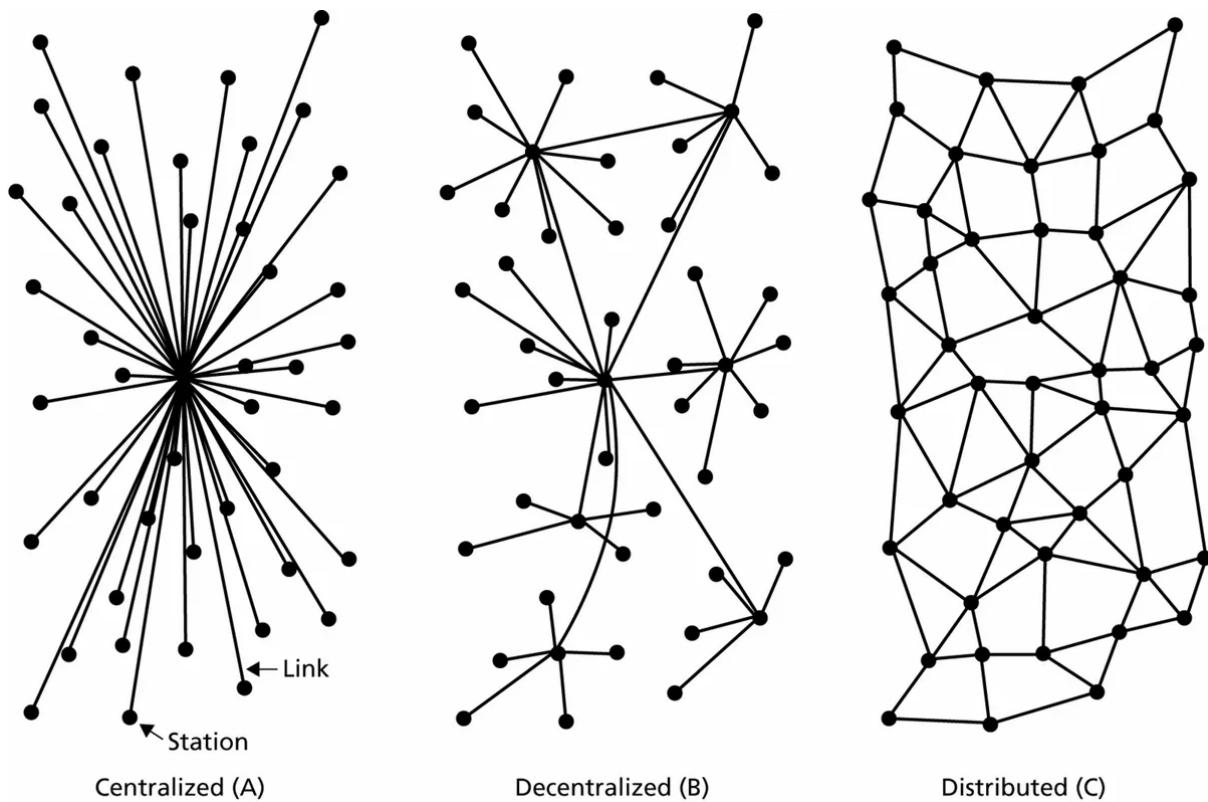
> **Roteamento dinâmico:** A internet usa algoritmos de roteamento dinâmico para rotear dados de um dispositivo para outro, permitindo uma comunicação eficiente e eficaz mesmo em caso de possíveis falhas ou congestionamento da rede.

> **Transparência:** A internet permite transparência na comunicação, pois, todos os dados são transmitidos abertamente e podem ser interceptados e monitorados por qualquer pessoa com as ferramentas apropriadas.

> **Alcance Global:** A internet tem alcance global, permitindo a comunicação e o acesso à informação de qualquer lugar do mundo.

Essas características, aliadas a outras como medidas robustas de segurança e suporte a uma ampla gama de aplicativos e serviços, fazem da internet a rede poderosa e dinâmica que é hoje.

> **Topologias de rede**



\*Diagrama de Paul Baran

Em 1964, o problema apresentado na nossa aula #1, já tinha sido imaginado e corrigido. Paul Baran apontou a fragilidade de modelos centralizados e propôs outros dois que podem ser utilizados para diferentes finalidades, o distribuído e o descentralizado.

Quando se tratam de dispositivos físicos, hardware, um modelo de rede distribuída permite a criação de sistemas de larga escala e altamente escaláveis que podem lidar com uma grande quantidade de dados e tráfego. Isso ocorre porque os dados podem ser distribuídos em vários dispositivos (nós), reduzindo erros em todos os pontos, tornando o sistema mais resistente a falhas enquanto mantém os dados amplamente disponíveis.

DAOs são uma tecnologia de organização que visa replicar o modelo de rede distribuída em um sentido de hierarquia. Essas organizações são projetadas para serem descentralizadas e administradas por código, em vez de serem controladas por uma autoridade central. O objetivo das DAO é criar um modelo organizacional mais democrático e transparente, onde as decisões sejam tomadas por consenso e a distribuição de poder seja diretamente proporcional à contribuição de cada indivíduo.

# Criptografia

## > O que é

Criptografia é a prática de proteger informações codificando-as de forma que só possam ser decifradas por indivíduos autorizados. Em termos mais simples, a criptografia é o método usado para tornar as informações confidenciais e acessíveis apenas para quem deveria vê-las.

Aqui está um exemplo simples de criptografia em ação:

Imagine que você tem uma mensagem que deseja enviar a um amigo, mas não deseja que mais ninguém a leia. Você pode usar uma forma simples de criptografia chamada cifra de substituição, em que cada letra da mensagem é substituída por outra letra ou símbolo. Por exemplo, você pode substituir cada letra na mensagem pela letra que vem três posições depois no alfabeto (A torna-se D, B torna-se E e assim por diante). Seu amigo seria então capaz de decodificar a mensagem invertendo a substituição.

## > EXEMPLO

Esse exemplo, apesar de muito básico, ilustra o conceito de como se usa criptografia para codificar uma mensagem de forma a torná-la confidencial e acessível somente a determinados indivíduos.

\*Para decifrar a mensagem, o destinatário simplesmente inverte a substituição, pegando cada letra três posições para trás no alfabeto\*

Mensagem original: "OLÁ MUNDO"

Mensagem cifrada: "RODÊ PXOW"

## > Crie um método de criptografia aqui:

## > CRIPTO.... MOEDA

A tecnologia Blockchain usa criptografia para proteger as transações financeiras, a confidencialidade e integridade das informações. Em uma transação de criptomoedas, a chave pública (endereço de carteira) do remetente criptografa a transação e a chave privada do destinatário a descriptografa, garantindo que apenas o destinatário possa acessar os dados, ou seja, o saldo.

## > Criptografia de chave simétrica e assimétrica

A criptografia de chave simétrica usa a mesma chave para criptografar e descriptografar informações. Isso significa que tanto o remetente quanto o destinatário das informações devem ter a mesma chave. Exemplos: AES e Blowfish.

A criptografia simétrica é rápida e eficiente, tornando-a adequada para criptografar grandes quantidades de dados. No entanto, tem a desvantagem de exigir que o remetente e o destinatário tenham acesso à mesma chave, o que pode ser difícil de gerenciar e proteger na prática.

A criptografia assimétrica, também conhecida como criptografia de chave pública, usa duas chaves diferentes para criptografar e descriptografar informações. Uma chave, chamada de chave pública, é usada para criptografar as informações, enquanto a outra chave, chamada de chave privada, é usada para descriptografá-las. Exemplos de criptografia assimétrica incluem RSA e criptografia de curva elíptica.

A criptografia assimétrica é adequada para situações em que não é prático compartilhar uma chave secreta, como em assinaturas digitais e comunicação

segura. Por exemplo, na comunicação segura, o remetente pode usar a chave pública do destinatário para criptografar a mensagem e o destinatário pode usar sua chave privada para descriptografá-la. A segurança do sistema é baseada no fato de que é computacionalmente inviável determinar a chave privada a partir da chave pública.

#### > Endereço de carteira, chave privada

Na Tecnologia Blockchain a chave pública é o endereço de carteira que você compartilha. Ele possui algumas dezenas de caracteres enquanto, a chave privada, tem centenas de caracteres, é usada para autenticar as transações, e, geralmente, é desconhecida pelo próprio usuário pois geralmente ela é gerenciada por um dispositivo (hard wallet), software ou serviço (exchanges).

Ao criar uma nova carteira na Metamask, por exemplo, o usuário tem acesso a uma sequência de 12 palavras que é uma maneira de restaurar sua carteira, porém, quem gerencia suas chaves privadas e permite que ele resgate sua carteira é o software.

## Como funciona a Blockchain

A Blockchain é um conjunto de tecnologias de registro distribuído, auditáveis, imutáveis e anônimos. Essas características fazem dela uma ferramenta extremamente útil, não apenas para armazenar valores monetários e validar transações, mas também para diversas outras aplicações. Muitas das quais sabemos e outras que ainda estão por serem descobertas!

#### > Para que é boa a Blockchain?

> **Criptomoedas:** A tecnologia Blockchain foi originalmente desenvolvida para dar suporte à criação de moedas digitais, como o Bitcoin.

> **Gerenciamento da Cadeia de Suprimentos (Supply Chain):** A Tecnologia Blockchain torna mais barato gerar confiança e, por consequência, maior transparência e eficiência no gerenciamento da cadeia de suprimentos.

- > **Identidade Digital:** A tecnologia Blockchain pode ser usada para criar identidades digitais seguras e descentralizadas, proporcionando aos usuários maior controle sobre seus dados pessoais permitindo que instituições possam validar processos sem ter acesso aos dados das pessoas.
- > **Contratos inteligentes:** Uma das aplicações mais notáveis da Tecnologia Blockchain é a criação de contratos autoexecutáveis, conhecidos como contratos inteligentes, que podem ser usados para automatizar processos complexos e reduzir o risco de fraude.
- > **Votação:** A Tecnologia Blockchain pode ser usada para criar sistemas de votação seguros e transparentes, permitindo eleições mais seguras e justas, além de modelos de governança mais descentralizados.
- > **Imóveis:** Cartórios 24 horas, operações conduzidas com segurança da sua casa.
- > **Sistema de saúde:** Armazenar e compartilhar registros médicos com segurança, melhorando a privacidade do paciente e permitindo uma prestação de cuidados com a saúde mais eficiente e eficaz.
- > **Organizações de caridade e sem fins lucrativos:** A Blockchain pode ser usada para aumentar a transparência e a responsabilidade em organizações de caridade e sem fins lucrativos, permitindo que os doadores rastreiem a distribuição de suas doações, bem como possam auditá-las, em tempo real, toda a atividade financeira da instituição.

## Como funciona a mineração do Bitcoin

A tecnologia Blockchain foi concebida para que o Bitcoin pudesse existir e, como ele foi a primeira criptomoeda e é a maior em capitalização de mercado até os dias de hoje, o processo de mineração dele também é uma referência para o mercado como um todo.

O que faz o Bitcoin especial, entre outras coisas, é o que se dá o nome de “estoque deflacionário”. Com uma mecânica oposta a do dinheiro das

instituições, como o real, euro e dólar, o Bitcoin tem limite de emissão: 21 milhões.

O processo ocorre em milhões de computadores espalhados pelo mundo e, apesar da rede ser bastante econômica, quando comparada ao gasto de energia nominal do sistema financeiro tradicional, tem um grande custo para aqueles que a mantém funcionando: os mineradores.

Através de um processo de tentativa e erro, os mineradores tentam adivinhar uma variável de uma equação para gerar uma espécie de código de barras que inicie com o maior número de zeros possível. A dificuldade da rede é ajustada pela quantidade mínima de zeros exigidos.

A cada 10 minutos, aproximadamente, um novo bloco com as últimas transações é gerado e a pessoa que decifra a hash (código único identificador, nosso código de barras) recebe a recompensa (novos Bitcoins). A cada 210 mil blocos a recompensa é diminuída pela metade. Esse evento se chama Halving e demora aproximadamente 4 anos.

> Dados usados para gerar a Hash

> **Transações:** os mineradores precisam incluir uma lista de transações recentes no bloco que estão minerando.

> **Header do bloco:** o Header do bloco inclui metadados sobre o bloco nem como um identificador de data/hora.

> **Nonce:** Um nonce é um número aleatório gerado pelo minerador e incluído no Header do bloco. O nonce é usado como o único dado que muda para variar a entrada a fim de encontrar uma hash que atenda ao alvo de dificuldade da rede.

> **Dificuldade alvo:** O alvo de dificuldade é um valor numérico definido pela rede que define o nível de complexidade necessário para que a hash seja válida. A meta de dificuldade se ajusta dinamicamente ao longo do tempo para manter o tempo médio entre a geração de blocos em 10 minutos.

> Hash do Bloco Anterior: Os mineradores precisam incluir a hash do bloco anterior da cadeia.

Uma vez que o minerador tenha a hash alvo, ele informa o nonce e todos os outros mineradores podem confirmar que ele resolveu a hash em primeiro lugar e merece receber a recompensa.

## AULA 4 Tipos de tokens aula 1: Principais tipos de tokens

O token é uma representação de alguma coisa que pode ser desde dinheiro até uma escritura de uma casa ou a uma saca de café.

Por conta das inúmeras ideias e objetos que podem e vão, eventualmente, ser representados dentro da Blockchain, temos diversos tipos de tokens.

### Diferença entre moeda e token

Nem todo projeto tem sua própria rede. Alguns projetos são construídos sob uma estrutura pré-existente e, para diferenciar, esses são chamados de tokens.

A Matic (polygon) é uma solução bastante curiosa por ser um token, construído para oferecer uma solução de escalabilidade para a rede Ethereum, porém o projeto tem também sua própria Blockchain. Como seu propósito é dar escalabilidade para a rede Ethereum, ela é, ainda assim, considerada um token mesmo tendo sua própria rede.

## Fungibilidade e não-fungibilidade

O ouro, sacas de café e carros são objetos fungíveis pois são substituíveis. Por exemplo, se eu pego 1kg de ouro em um empréstimo eu não preciso devolver “o mesmo” quilo de ouro pois, desde que seja da mesma qualidade (24k, por exemplo), esse quilo é igual a qualquer outro.

Além disso, objetos fungíveis tendem a ser divisíveis. Um bom exemplo é o dinheiro ou o próprio Bitcoin. Se eu tenho uma nota de 50 ela pode ser trocada por 5 de 10, por exemplo, bem como se eu tenho 1 BTC inteiro eu posso mandar apenas uma fração dele, digamos, 0,05, por exemplo.

Porém existem alguns objetos que não possuem essa propriedade, por exemplo, uma casa. Por mais que possa haver outra com o mesmo tamanho, ou quaisquer outros atributos que seja, uma casa é inteiramente única e insubstituível. Da mesma maneira uma música ou um quadro possuem essa mesma características e, por isso, na hora de representar esses objetos como artigos digitais precisamos de um tipo específico de token, os Tokens Não-fungíveis.

## Tokens não fungíveis

Os NFTs, ou seja, token não fungíveis (Non Fungible tokens) foram criados exatamente com o propósito de termos alguma maneira de representar ideias e coisas como músicas, escrituras/documentos, itens colecionáveis e até domínios.

## Smart contracts

Contratos inteligentes ou smart contracts são códigos armazenados e executados na Blockchain que, quando certas condições pré-estabelecidas

acontecem, se executam automaticamente. Um exemplo comum mas desconhecido é o próprio NFT que é um tipo de smart contract.

## Principais tipos tokens/moedas

O tempo todo surgem projetos e, como maneira de diferenciar o funcionamento e objetivo, acabaram criando vários tipos diferentes de tokens.

- > **Utility Tokens** - São tokens que concedem acesso a produtos e serviços em uma plataforma específica. Eles são usados para recompensar usuários e incentivar o uso da plataforma. Exemplo: Binance Coin (BNB).
- > **Security Tokens** - São tokens que representam um ativo, como ações ou títulos, e são regulamentados pelas autoridades financeiras. Eles oferecem a capacidade de investir em um ativo sem a necessidade de um intermediário financeiro tradicional. Exemplo: tZero (TZRO).
- > **Payment Tokens** - São tokens usados para transações de pagamento e são normalmente usados para substituir as moedas tradicionais. Exemplo: Bitcoin (BTC).
- > **Asset-Backed Tokens** - São tokens que representam um ativo físico, como ouro, prata, petróleo ou imóveis. Eles fornecem exposição aos preços desses ativos sem a necessidade de comprá-los fisicamente. Exemplo: Paxos Gold (PAXG).
- > **Governance Tokens** - São tokens usados para governança e decisões sobre o futuro da plataforma. Os detentores desses tokens têm direito a voto em questões importantes. Exemplo: Maker (MKR).
- > **Non-Fungible Tokens (NFTs)** - São tokens usados para representar ativos únicos e não substituíveis, como obras de arte digitais, itens colecionáveis e jogos virtuais além de poderem ser usados para representar ativos que existem também na vida real como carros colecionáveis. Exemplo: CryptoKitties.

> **Stablecoins** - São tokens que possuem um valor fixo, normalmente atrelado a uma moeda fiduciária, como o dólar americano. Eles são usados para facilitar a entrada e saída do mercado de criptomoedas. Exemplo: Tether (USDT).

## Principais projetos

> **BTC (Bitcoin)**: A primeira criptomoeda a ser lançada, possui a maior capitalização de mercado. Foi lançado em 2009 e é uma moeda digital descentralizada que opera nos computadores dos usuários através de um mecanismo de consenso de prova de trabalho (PoW). BTC é a criptomoeda nativa da rede Bitcoin e é usada para transações, como reserva de valor e para fins de investimento, além de ser a referência do mercado de criptomoedas.

> **ETH (Ethereum)**: Lançado em 2015, o Ethereum é um projeto de um “computador do mundo”, uma plataforma blockchain descentralizada que permite a criação de contratos inteligentes e aplicativos descentralizados (DApps). A criptomoeda nativa da rede Ethereum é o Ether (ETH), que é usado para medir o gasto computacional das aplicações dentro da rede e pagar taxas de transação.

> **USDT (Tether)**: Lançado em 2014, o Tether é uma stablecoin atrelada ao dólar americano. O USDT é usado para facilitar a negociação de criptomoedas nas exchanges e fornecer uma reserva estável de valor para os usuários.

> **BNB (Binance Coin)**: Lançado em 2017 pela Binance, uma das maiores exchanges de criptomoedas, o BNB é utilizado como um token de utilidade na plataforma tanto para pagar taxas mais baratas de transação como acessar recursos avançados de negociação e participar das vendas e distribuições de tokens do Launchpad da plataforma.

> **USDC (USD Coin)**: Lançado em 2018, o USDC é uma stablecoin atrelada ao dólar americano. Ele é emitido pela Circle juntamente com a Coinbase que é a maior exchange norte americana.

> **BUSD (Binance USD)**: Lançado em 2019, o BUSD é uma stablecoin atrelada ao dólar americano emitida pela Binance.

> **XRP (Ripple)**: Lançado em 2012, o XRP é a criptomoeda nativa da rede Ripple. O XRP é usado para facilitar pagamentos internacionais rápidos e de baixo custo, fornecendo liquidez às instituições financeiras enquanto funciona como moeda de câmbio similar ao dólar no cenário de câmbio global.

> **ADA (Cardano)**: Lançado em 2017 por um co-fundador da Ethereum (Charles Hoskinson), é a criptomoeda nativa da plataforma blockchain Cardano. A ADA é usada para pagar taxas de transação e participar da governança da rede Cardano.

> **DOGE (Dogecoin)**: Lançada em 2013 como uma brincadeira, a Dogecoin é uma criptomoeda descentralizada que opera em um mecanismo de consenso PoW. É a primeira meme coin e tem natureza bastante especulativa.

> **MATIC (Polygon)**: Lançado em 2019, MATIC é a criptomoeda nativa da rede Polygon, que é uma solução de escalonamento de Camada 2 para Ethereum. A MATIC é usada para pagar taxas de transação, participar da governança da rede e acessar alguns recursos.

> **DOT (Polkadot)**: Lançado em 2020, DOT é a criptomoeda nativa da plataforma blockchain Polkadot. O DOT é usado para participar da governança da rede e para acessar recursos avançados.

> **DAI (Dai)**: Lançado em 2017, o Dai é uma stablecoin algorítmica atrelada ao dólar americano.

> **LTC (Litecoin)**: Lançado em 2011, o Litecoin é uma criptomoeda descentralizada que opera em um mecanismo de consenso PoW.

> **SHIBA (Shiba Inu)**: Lançado em 2020, Shiba Inu é uma meme coin que opera em um mecanismo de consenso PoW. Foi lançada com a ideia de destronar a Dogecoin.

> **SOL (Solana):** Solana é uma blockchain proof-of-stake (PoS) que foi lançada em março de 2020. SOL é o token nativo da rede Solana e é usado para taxas de transação e recompensas para investidores. A Solana visa fornecer uma plataforma blockchain de alto desempenho que pode suportar aplicativos descentralizados (dApps) e outros casos de uso.

> **TRX (TRON):** TRON é um sistema operacional baseado em blockchain que foi lançado em 2017. TRX é o token nativo da rede TRON e é usado para taxas de transação e outros fins dentro do ecossistema TRON. O projeto visa fornecer uma plataforma para o desenvolvimento de aplicativos descentralizados e distribuição de conteúdo.

> **UNI (Uniswap):** Uniswap é uma exchange descentralizada (DEX) que foi lançada em 2018. UNI é o token de governança do protocolo Uniswap e é usado para a tomada de decisões relacionadas ao desenvolvimento e gerenciamento do protocolo. A Uniswap é baseada no modelo de criador de mercado automatizado (AMM) e foi projetada para permitir a negociação de criptomoedas de maneira descentralizada, sem nenhuma entidade que controle suas operações

> **LINK (Chainlink):** Chainlink é uma rede oracle descentralizada que foi lançada em 2017. LINK é o token nativo da rede Chainlink e é usado para pagar solicitações de dados e outros serviços prestados pela rede. A Chainlink visa fornecer um mecanismo seguro e confiável para conectar contratos inteligentes baseados em blockchain a dados e serviços fora da rede blockchain.

> **XMR (Monero):** Criptomoeda focada em privacidade que foi lançada em 2014. XMR é usado para transações e para pagar taxas de rede. O Monero é baseado em um mecanismo de consenso de prova de trabalho (PoW) e foi projetado para fornecer fortes recursos de privacidade e anonimato.

> **BCH (Bitcoin Cash):** é uma criptomoeda que foi criada em 2017 como resultado de um hard fork da blockchain original do Bitcoin. O BCH é usado para transações e para pagar taxas de rede. O Bitcoin Cash visa fornecer transações mais rápidas e baratas do que o Bitcoin, aumentando o limite de tamanho do bloco.

> **XTZ (Tezos)**: Tezos é uma plataforma blockchain PoS lançada em 2018. XTZ é o token nativo da rede Tezos e é usado para taxas de transação e recompensas. A Tezos visa fornecer uma blockchain autocorrigível que pode evoluir ao longo do tempo por meio da governança on-chain.

> **PAXG (Paxos Gold)**: é um token lastreado em ativos que representa uma onça de ouro físico armazenado em um cofre seguro. O PAXG foi lançado em 2019 e é baseado na blockchain Ethereum. O PAXG foi projetado para fornecer uma maneira conveniente para os investidores obterem exposição ao preço do ouro sem precisar armazenar fisicamente o metal.

> **DASH**: Dash é uma criptomoeda lançada em 2014. DASH é usada para transações e para pagar taxas de rede. A Dash visa fornecer transações mais rápidas e privadas do que o Bitcoin usando uma rede de dois níveis que combina PoW e masternodes.

> **BAT (Basic Attention Token)**: Token de utility usado no navegador Brave para recompensar os usuários por visualizar anúncios e pagar por conteúdo premium. O BAT foi lançado em 2017 e é baseado na blockchain Ethereum. A Brave tem como objetivo fornecer um modelo de publicidade online mais privado e eficiente que beneficie usuários e editores.

> **MANA (Decentraland)**: Decentraland é um mundo virtual lançado em 2017. MANA é o token nativo do ecossistema Decentraland e é usado para comprar e vender terras virtuais e outros ativos digitais. Decentraland é baseada na blockchain Ethereum e foi projetada para fornecer uma plataforma descentralizada para construir e experimentar aplicativos de realidade virtual.

## Principais redes

> **Bitcoin (BTC)**: A primeira criptomoeda, projetada para ser uma moeda digital global descentralizada e segura. Atualmente, mais de US\$92 bilhões estão alocados em Bitcoin.

> **Ethereum (ETH)**: Uma plataforma de contrato inteligente que permite que desenvolvedores criem aplicativos descentralizados (dApps) e tokens

personalizados. O valor total alocado no Ethereum é de cerca de US\$55 bilhões.

- > **Binance Smart Chain (BSC):** Uma blockchain rápida e escalável que oferece compatibilidade com contratos inteligentes da Ethereum. A BSC tem mais de US\$12 bilhões alocados.
- > **Cardano (ADA):** Uma plataforma de contratos inteligentes que visa fornecer uma solução escalável, interoperável e sustentável para dApps e tokens personalizados. O valor total alocado na Cardano é de cerca de US\$6 bilhões.
- > **Polkadot (DOT):** Uma plataforma de interoperabilidade que permite a transferência de dados e ativos entre diferentes blockchains. Atualmente, cerca de US\$30 bilhões estão alocados na Polkadot.
- > **Solana (SOL):** Uma blockchain de alto desempenho que oferece um ambiente para desenvolvedores criarem aplicativos escaláveis e de alto desempenho. O valor total alocado na Solana é de cerca de US\$7 bilhões.
- > **Avalanche (AVAX):** Uma plataforma de contratos inteligentes que visa oferecer escalabilidade, interoperabilidade e segurança para a criação de dApps. O valor total alocado na Avalanche é de cerca de US\$5 bilhões.
- > **Chainlink (LINK):** Uma rede de um oráculo descentralizada que fornece informações externas para contratos inteligentes em várias blockchains. Atualmente, cerca de US\$17 bilhões estão alocados em Chainlink.
- > **Polygon (MATIC):** Uma plataforma de escalabilidade que oferece compatibilidade com contratos inteligentes da Ethereum. O valor total alocado na Polygon é de cerca de US\$9 bilhões.
- > **Uniswap (UNI):** Uma plataforma de negociação descentralizada (DEX) que permite que usuários negoçiem tokens diretamente de suas carteiras. Atualmente, mais de US\$4 bilhões estão aloados na Uniswap.
- > **Cosmos (ATOM):** Uma plataforma de blockchain que permite a interoperabilidade entre blockchains e aplicativos descentralizados. O valor

total alocado na rede Cosmos é de cerca de US\$3 bilhões.

- > **Algorand (ALGO):** Uma plataforma de blockchain que oferece velocidade, segurança e escalabilidade para a criação de aplicativos descentralizados. O valor total alocado na Algorand é de cerca de US\$2 bilhões.
- > **Tezos (XTZ):** Uma plataforma de contratos inteligentes que oferece governança descentralizada e atualizações sem interrupções. O valor total alocado na rede Tezos é de cerca de US\$1 bilhão.

## Como stablecoins são pareadas (peg)

A paridade das stablecoins não é perfeita e sofre leves flutuações o tempo todo e existem casos, inclusive, de stablecoins que perderam a paridade (peg) com o dólar.

### > Stablecoins com lastro em moeda fiduciária(fiat):

Estas são lastreadas por uma reserva de moeda fiduciária mantida por um custodiante. Para cada unidade de stablecoin emitida, o emissor deve deter uma quantidade correspondente de moeda fiduciária em uma conta bancária ou reserva. O valor da stablecoin é sustentado pela reserva do ativo subjacente. Assumindo que a quantidade seja igual ou maior ao total de stablecoins emitidas está tudo certo, porém, caso seja auditado e aconteça de as reservas serem menores do que o total de tokens emitidos, a moeda pode perder a confiança e por consequência o lastro.

Exemplos:

- > **Tether (USDT):** Tether é uma stablecoin que está ligada ao dólar americano. Para cada USDT emitido, a Tether Limited, teoricamente, detém uma quantidade equivalente de dólares americanos em suas reservas.
- > **USD Coin (USDC):** USDC é uma stablecoin que também está ligada ao dólar americano. A stablecoin é emitida pela Circle, que mantém reservas de dólares americanos para respaldar a stablecoin.

### > Stablecoins com lastro em criptomoedas:

As stablecoins com lastro em criptomoedas são lastreadas por uma reserva de criptomoedas, como Bitcoin ou Ether. O valor da stablecoin é mantido garantindo que a reserva de criptomoedas seja igual ao valor total das stablecoins emitidas. Exemplos de stablecoins com lastro em criptomoedas incluem:

> **Dai (DAI)**: DAI é uma stablecoin que está ligada ao dólar americano e é lastreada por uma reserva de garantia baseada principalmente em criptomoedas mas não deixa claro, qual é a colateralização. Os usuários podem depositar Ethereum ou outras criptomoedas como garantia para criar DAI, que eles podem então usar como stablecoin.

> **BitUSD**: BitUSD é uma stablecoin que está ligada ao dólar americano e é lastreada por uma reserva de criptomoedas BitShares. Os usuários podem depositar BitShares como garantia para criar BitUSD, que eles podem usar como stablecoin.

### > Stablecoins algorítmicas:

As stablecoins algorítmicas não são lastreadas por nenhum ativo subjacente, mas em vez disso usam uma abordagem algorítmica para manter seu valor. O algoritmo ajusta o suprimento da stablecoin com base na demanda do mercado e outros fatores para manter sua ligação a um ativo específico.

Exemplos:

> **Ampleforth (AMPL)**: Ampleforth é uma stablecoin algorítmica que é projetada para manter seu valor em termos de poder de compra em vez de um ativo específico. O protocolo ajusta automaticamente o suprimento de AMPL com base na demanda do mercado para manter seu preço-alvo.

> **Frax (FRAX)**: Frax é uma stablecoin algorítmica que é projetada para estar ligada ao dólar americano. O protocolo usa um algoritmo complexo para ajustar o suprimento de FRAX com base na demanda do mercado e outros fatores para manter sua ligação.

### > Stablecoins com garantia de commodities:

As stablecoins garantidas por commodities são lastreadas por uma reserva de uma commodity física, como ouro, prata ou petróleo. O valor da stablecoin é mantido garantindo que a reserva da mercadoria subjacente seja igual ao valor total das stablecoins emitidas. Exemplos de stablecoins com garantia de commodities incluem:

- > **Digix Gold Token (DGX):** DGX é uma stablecoin que está atrelada ao preço do ouro. Para cada DGX emitido, a Digix mantém uma quantidade correspondente de ouro em reserva.
- > **Paxos Standard (PAX):** PAX é uma stablecoin atrelada ao dólar americano e lastreada por uma reserva de uma combinação de caixa e equivalentes de caixa, títulos do Tesouro dos EUA de curto prazo e outros títulos de dívida de grau de investimento de curto prazo.

## Perigos das stable coins - história da luna

As stablecoins são indispensáveis no mercado cripto, porém existem preocupações sobre a estabilidade desses ativos e seu potencial impacto em todo o mercado financeiro.

Em 2019, a Terra (Luna) atraiu o interesse de investidores e empresas, incluindo a Three Arrows Capital, que investiu significativamente na criptomoeda. Em 2022, no entanto, a Terra Luna sofreu um grande crash, que foi o ponto de partida para o subsequente crash da FTX (exchange associada a Three Arrows Capital).

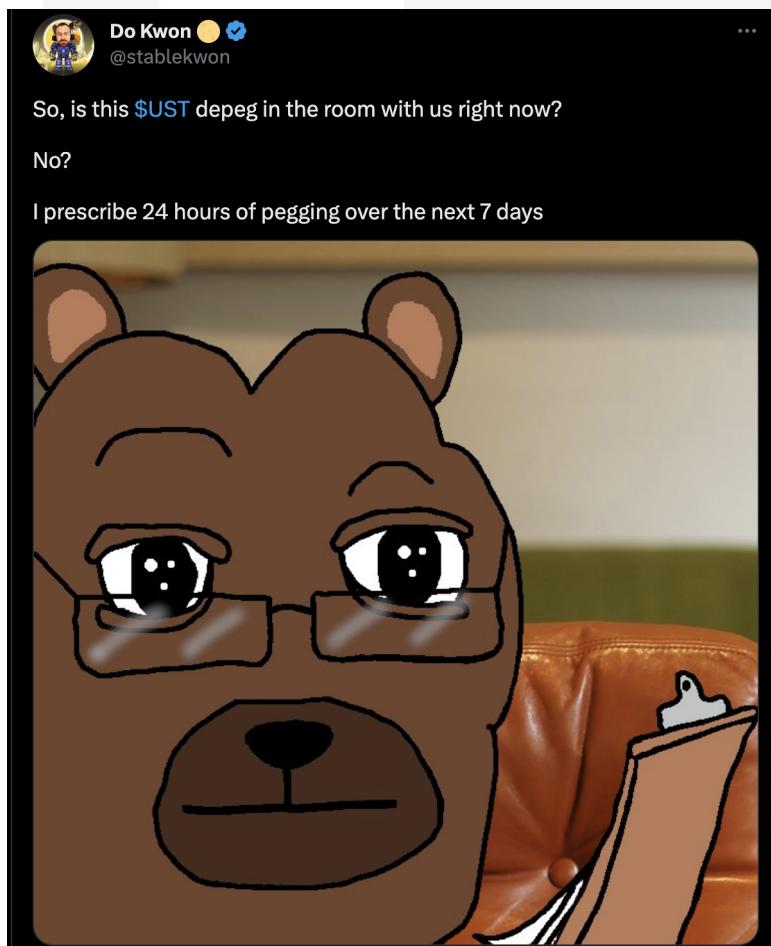
A mecânica do projeto fazia com que usuários queimassem o token nativo para gerar UST, uma moeda estável pareada no dólar e podiam empregar esse capital tanto para negociar como para ganhar rendimentos. Porém o caminho reverso, ou seja, devolver o UST, acabava criando novas moedas.

Como o valor de um ativo é precificado de acordo com a oferta e procura, enquanto os investidores procuravam investir no projeto os preços aumentavam substancialmente, porém quando o preço ultrapassou os 80

dólares e aconteceu o recorde de menor circulação do token, uma moeda com um sistema parecido (WAVES) enfrentou um colapso por falta de confiança.

Não demorou muito para que os investidores percebessem o problema da Terra (LUNA) e, não muito tempo depois disso, começaram a se desfazer da stablecoin UST em grandes quantidades, o que fez com que a moeda perdesse o lastro. Momentaneamente Do Kwon, fundador, brincou com isso em seu twitter

Porém uma vez que o preço caiu de US\$0,98 por unidade uma boa parte dos investidores começaram a se desfazer dos tokens fazendo com que o valor do UST e da LUNA despencassem 99% em aproximadamente 24 horas.



Brincadeira ou falta de responsabilidade?

# AULA 5 - Tipos de tokens aula 2: NFTs, governança e maluquice

## O que é NFT então?

Foi dito anteriormente que os NFTs são representações digitais de algo que não é divisível e substituível, ou seja, que é único e indivisível como um imóvel, uma escritura ou até uma obra de arte.

Na prática isso reflete em um novo padrão de tokens. Os padrões mais usados para tokens não fungíveis são ERC-721 e ERC-1155. Apesar da ideia original nossa concepção parte do mais popular que, geralmente, são coleções ou artigos de jogos porém, o que nos interessa nesse módula, é a tecnologia.

> **ERC-721:** Ao contrário dos tokens fungíveis (ERC-20), que são armazenados em uma matriz unidimensional, os tokens ERC-721 são armazenados em uma estrutura de dados chamada árvore de Merkle. Isso permite que os tokens sejam organizados em uma hierarquia, tornando mais fácil pesquisar, exibir e transferir ativos digitais únicos. Além disso, o padrão ERC-721 permite que os proprietários dos NFTs sejam facilmente identificados, rastreados e gerenciados.

Os tokens ERC-721 são tipos de contratos inteligentes na blockchain Ethereum. Cada token é um contrato que é registrado na blockchain. O contrato contém todas as informações sobre o NFT, incluindo seu proprietário atual, o histórico de transações e outras informações relevantes.

A rede Ethereum gerencia automaticamente todas as transações envolvendo tokens ERC-721, garantindo que o proprietário atual do NFT tenha permissão para transferi-lo.

O padrão ERC-721 também inclui uma série de funções que podem ser usadas para gerenciar e transferir NFTs. Por exemplo, a função "approve" permite que um proprietário de token autorize outro usuário a transferir o NFT em seu nome. A função "transferFrom" permite que o proprietário atual

do NFT transfira o token para outro usuário. Além disso, os desenvolvedores podem criar funções personalizadas para adicionar funcionalidades exclusivas aos seus NFTs.

> **ERC-1155:** Esse contrato inteligente permite que um único contrato represente várias instâncias de tokens fungíveis e não-fungíveis. Esses tokens podem ser negociados em massa, transferidos em lotes e gerenciados de forma eficiente usando uma única transação.

Ao contrário do padrão ERC-721, que permite a criação de tokens não fungíveis, cada um com uma identidade única, o padrão ERC-1155 permite a criação de tokens que podem ser fungíveis ou não-fungíveis, ou uma combinação de ambos.

Cada instância de token ERC-1155 é identificada por um ID de token exclusivo, que é usado para identificar e diferenciar entre tokens. A identidade de cada token pode ser determinada por meio da consulta do ID de token correspondente em uma função de leitura no contrato inteligente. Além disso, o contrato inteligente pode definir vários atributos para cada tipo de token, incluindo o nome, símbolo, número total de tokens e metadados associados.

O padrão ERC-1155 também oferece recursos avançados de segurança e privacidade, como a capacidade de limitar o acesso a determinados tokens ou criar tokens com diferentes níveis de permissão para diferentes usuários.

## Colecionáveis não erc-721

Antes da criação do ERC-721 e ERC-1155, os tokens não fungíveis (NFTs) existiam em várias formas, inclusive na blockchain do Bitcoin usando uma técnica chamada colored coins (moedas coloridas). O método era usado para representar tokens únicos vinculados a bens ou bens específicos. Os tokens foram criados “colorindo” uma fração de um bitcoin com metadados, criando assim um ativo novo e único. No entanto, esse método não foi projetado especificamente para NFTs e havia limitações quanto aos tipos de ativos que poderiam ser representados.

Outro método pré-ERC-721 de criação de NFTs foi a plataforma Counterparty, que foi construída sobre a blockchain do Bitcoin. A Counterparty permitiu que os usuários criassem tokens personalizados que eram exclusivos e representavam ativos específicos. Esta plataforma foi usada para criar uma variedade de NFTs, incluindo cartas raras para o popular jogo de cartas online, Spells of Genesis.

Além de colored coins(moedas coloridas) e Counterparty, também havia vários outros métodos usados para criar NFTs antes da introdução do ERC-721 e ERC-1155. Por exemplo, em 2014, o desenvolvedor do jogo, Rare Pepe Wallet, criou uma coleção de NFTs chamada "Rare Pepes". Esses tokens foram criados usando a blockchain do Bitcoin, com cada token representando uma imagem única de um sapo de desenho animado. A popularidade do Rare Pepes levou à criação de várias outras coleções NFT, incluindo a coleção "CryptoKitties", que foi construída na blockchain Ethereum e lançada em 2017, também antes da criação dos padrões discutidos.

### **Para que servem e para que não servem os NFTs!**

Apesar de padrões e referências, os melhores usos para NFTs ainda estão por surgir. O BAYC (Bored Ape Yatch Club) é extensamente aclamado e criticado por, ao mesmo tempo que se tornou extremamente conhecido e valioso, dar indícios de jogar sujo e usar estratégias de front running, antecipando-se a suas próprias transações, controlar o supply de seu token no lançamento para que ele inflasse de preço artificialmente e, a acusação mais séria, é que, a empresa teria pago as celebridades como Neymar, Madonna, Justin Bieber e Shop Dog, entre outros, para serem holders de seus NFTs e divulgarem seus NFTs. Isso sem mencionar quantas pessoas não perderam dinheiro comprando NFTs para participar de jogos Play-to-earn como axie infinity.

Tudo isso dito, fica muito nítida a impressão de que NFTs são figurinhas ou itens colecionáveis e geralmente ligados a modelos de negócios duvidosos ou, ao menos, falhos.

Os NFTs tem aplicações excelentes que são quase completamente ignoradas, como permitir a venda direta de músicas de artistas para fãs e/ou

a criação e distribuição de conteúdo/experiências exclusivas. Através da plataforma royals.io qualquer um pode participar no recebimento de royalties enquanto ajuda artistas, comprando um fragmento de suas obras.

Criar comunidades é importante e, apesar das críticas, BAYC conseguiu fazer isso muito bem! Esse é um uso importante dos NFTs porém também podem ser usados como lembranças virtuais de eventos, como foram as pulseiras NFT do Rock in Rio ou até, podemos imaginar usos inteiramente novos usando as características do padrão ERC-1155, por exemplo.

## Soulbound/PFP

> Soulbound: É um NFT que é permanentemente anexado a um endereço de blockchain ou wallet/carteira específica. Isso significa que o NFT não pode ser transferido para nenhuma outra carteira. Os NFTs Soulbound tem a idéia de soul = alma e bound = vínculo para que, mesmo com os dispositivos de privacidade possamos validar, inclusive, o caráter e confiabilidade daquele usuário trazendo uma camada extra de profundidade para a blockchain e até uma responsabilidade maior para os usuários.

> PFP: significa "imagem de perfil"(profile picture) e refere-se a um tipo específico de NFT usado para representar o avatar ou a imagem do perfil de um usuário. Os NFTs PFP podem ser comprados e vendidos em vários marketplaces e são frequentemente usados como uma forma de colecionável digital.

## Governança

Um dos desafios que a ideologia por trás do Bitcoin trás é a distribuição do poder. No caso, tudo começou com a moeda digital que, efetivamente, é uma prova de conceito da própria tecnologia Blockchain.

Com o avanço da aplicação dessa tecnologia temos um embate: Vamos repetir os erros que o Bitcoin veio para resolver? O mercado de criptomoedas ainda é extremamente dependente de exchanges que são, basicamente, o banco das criptomoedas. O que completamente ignora o

conceito/lema do Bitcoin, SEJA SEU PRÓPRIO BANCO!

Se consolida então, como dificuldade prática dessa ideologia, fomentar modelos com governança mais saudável, ou seja, distribuída, que respeite os ideais e fundamentos da tecnologia além do modelo de topologia de rede.

Os tokens de governança são ativos digitais usados para representar a propriedade e o controle de projetos descentralizados. Eles permitem que os detentores participem dos processos de tomada de decisão que regem o protocolo ou DAO, como votar em propostas de alterações no protocolo ou nas regras, gerenciar o tesouro(treasure) ou eleger representantes para governar a organização.

Na prática, os tokens de governança funcionam usando um sistema de contratos inteligentes para gerenciar os direitos de voto. Quando um usuário adquire tokens de governança, ele ganha a capacidade de participar dos processos de tomada de decisão do projeto ou DAO.

O processo de governança normalmente envolve uma série de propostas apresentadas por membros da comunidade. As propostas podem estar relacionadas a mudanças no código do protocolo, modificações no próprio sistema de governança ou pedidos de financiamento da tesouraria da organização. Depois que uma proposta é enviada, os detentores de tokens podem votar nela e a proposta é aceita ou rejeitada com base no resultado da votação.

O desafio do processo de governança é agir como projetado e realmente ser transparente e democrático, com cada detentor de token tendo voz igual no processo de tomada de decisão.

## **Representação De ativos da vida real**

A representação de ativos ou objetos do mundo real em uma blockchain como tokens é uma tendência. O processo mais comum é representar esse token através de um NFT e alguma empresa em país com legislação favorável fazer a custódia da propriedade e do NFT para que ele possa ser gerenciado como uma representação daquele ativo físico.

Tokenizar um ativo permite ao proprietário dividir ele em unidades menores que podem ser negociadas mais facilmente. Esse processo tem o potencial de aumentar a liquidez, reduzir os custos de transação e tornar modelos de investimento em, por exemplo, propriedades extremamente caras, mais acessíveis a uma gama mais ampla de investidores.

Além disso, a tokenização também proporciona um maior nível de transparência e segurança. Ao registrar a propriedade do ativo em um blockchain, a propriedade do ativo pode ser facilmente verificada e as transações podem ser rastreadas em tempo real.

## AULA 6 - Tudo o que você precisa saber sobre whitepaper

### O que é um whitepaper?

Um whitepaper deve ser um documento técnico, persuasivo e informativo que busca educar e informar um público (geralmente, pesquisadores e investidores) sobre um projeto, apresentando uma visão e soluções possíveis para um problema.

O documento descreve detalhadamente a estratégia de uma empresa ou organização, sua organização, arquitetura e segurança, e fornece informações técnicas e de negócios sobre um projeto de rede blockchain e/ou criptomoeda ou token, incluindo seu tokenomics e estratégias de desenvolvimento bem como prazos (road map).

Como o objetivo é convencer os leitores de que a tecnologia, produto ou serviço é valioso e que vale a pena investir tempo e recursos para desenvolvê-lo é importante avaliar em miúdos principalmente o objetivo e destino dos fundos levantados. Em muitos casos, o whitepaper é usado como um meio para arrecadar fundos por meio de uma oferta inicial de moedas (ICO, initial coin offering) ou de uma oferta inicial de tokens (ITO, initial token offering).

## **Por que é tão importante?**

A maioria dos projetos não oferece solução nenhuma e a maioria dos “investidores” nem sequer leem os whitepapers. 90% de todos os golpes e perdas de capital podem ser evitadas lendo o whitepaper e identificando padrões potencialmente perigosos, que já deram errado.

Existe até quem diz que não lê o whitepaper e vai direto na comunidade. A comunidade do projeto jamais deve ser dispensada porém algumas das maiores comunidades já tiveram baixas absurdas como o próprio projeto Terra(LUNA) e a própria exchange FTX que, até então, tinha um discurso extremamente altruísta, bonito e, inclusive, fazia como as grandes empresas internacionais e investia em lobby.

A lição é: Todo cuidado é pouco e, quando a matéria é investimentos e novas tecnologias, a chance de perder dinheiro é muito grande até por que a grande maioria das pessoas sequer entendem as soluções quanto mais as tecnologias e potenciais dificuldades de implementá-la e, quem dirá, avaliar a fundo um modelo econômico. A grande maioria das pessoas compra “a moedinha que está subindo” ou “aquela que meu amigo disse” e, mesmo com grandes retornos, não configura modelo de investimento e sim de aposta, ou seja, se você não estiver pensando em investir e ter retornos certos, estiver colocando o dinheiro para perder MESMO, nem precisa ler e analisar o whitepaper, comunidade, modelo econômico e time/roadmap.

## **Como ler um whitepaper resumidamente**

Para ler um whitepaper e abstrair as informações importantes você deve responder as perguntas/analisar e/ou coletar as informações abaixo:

1. Por que o projeto existe? A solução é viável?
2. Existe utilidade real?
3. Qual é o mecanismo de consenso utilizado?

4. Como o supply foi/será distribuído, qual o modelo econômico adotado?
5. Quem são os envolvidos?
6. Road Map
7. Comunidade

## As principais partes do whitepaper

- > **Abstract (Resumo):** Breve visão geral do projeto e sua finalidade.
- > **Introduction (Introdução):** Explicação do problema que a criptomoeda está tentando resolver e como ela difere das soluções existentes.
- > **Aspectos técnicos:** Descrição da tecnologia subjacente, incluindo o mecanismo de consenso, métodos de criptografia e outros detalhes técnicos, bem como dificuldades de implementação.
- > **Casos de uso:** Aplicações do mundo real para a criptomoeda/token, incluindo seu potencial para interferir nas indústrias tradicionais otimizando processos ou causando total disruptão deles.
- > **Economia (Tokenomics):** Esse segmento deve conduzir uma discussão sobre o modelo econômico da criptomoeda, incluindo seu fornecimento máximo (supply), se/como são gerados (minted, mintados) novos tokens, distribuição das moedas até o presente momento e gerenciamento do investimento captado.
- > **Road Map (Roteiro):** Plano para o desenvolvimento e implementação da criptomoeda.
- > **Equipe:** informações sobre a equipe por trás da criptomoeda, incluindo seus antecedentes e qualificações.
- > **Conclusão:** um resumo dos principais recursos e benefícios da criptomoeda, bem como quaisquer riscos ou desafios potenciais.

## Como funcionam modelos econômicos

Tokens são representações digitais de alguma coisa e podem representar propriedades, valores ou quaisquer outros ativos. Esses tokens podem ser negociados em mercados descentralizados, que operam sem a necessidade de intermediários como bancos ou outras instituições financeiras.

A tokenização pode ser um modelo mais eficiente e transparente de gerenciar sistemas econômicos, usando a tecnologia blockchain para facilitar transações e criação de confiança através da criação de registros imutáveis. Com a gestão do código é muito mais barato manter um sistema seguro do que em instituições tradicionais.

Os modelos econômicos tokenizados podem ser aplicados a uma ampla gama de atividades econômicas, desde imóveis e arte até propriedade intelectual e até mesmo conteúdo digital. Em cada caso, os tokens representam propriedade ou acesso a um ativo ou serviço específico e podem ser negociados em um mercado descentralizado.

Porém, o funcionamento da maioria dos projetos deixa a desejar na área do modelo econômico, principalmente por não apresentarem soluções reais, ou não terem um modelo econômico no qual o token se beneficia e captura o valor que gera.

Além disso, existem projetos e empresas que emitem tokens para recompensar usuários os quais não tem utilidade alguma e, por isso, não tem motivo para serem comprados uma vez que o usuário vende para recobrar a “recompensa”.

## História do Axie Infinity

Um dos maiores sucessos e fracassos que exemplifica tudo que há de errado no play-to-earn e usa NFTs de uma maneira duvidosa, é o Axie Infinity. O sistema passou por inúmeras mudanças após um crash EXTREMAMENTE previsível que ocorreu justamente por que a grande maioria das pessoas não entendem os conceitos presentes **NESTE MATERIAL!**

No auge, a dinâmica do jogo era a seguinte:

(fora os valores que foram necessários para se começar no jogo nada impedia o jogador de seguir ambas trilhas)

### > FARM

- 1 - O player comprava ao menos 3 NFTs de personagens (axies) para jogar;
- 2 - O player passava a cumprir missões que davam uma recompensa diária + recompensa para cada fase que o jogador completava, o fator limitante era a ENERGIA que dependia da quantidade de axies que a pessoa possuía.
- 3 - O player passava a ganhar SLP diariamente de acordo com algumas normas;
- 4 - O player vendia SLP no mercado para ganhar dinheiro;

### > BREED (reprodução)

- 1 - O player comprava pares de axies para eles procriarem;
- 2 - O player necessitava dos axies, SLP e AXS para criar novos axies;
- 3 - Ele os vendia no mercado para ganhar dinheiro;

Para pessoas pouco experientes ou com pouco entendimento de lógica talvez o problema não esteja tão aparente. Porém duas dinâmicas se construíram a partir desse modelo econômico:

- 1 - Os players/investidores mais experientes perceberam que a moeda para se ter em mãos era o AXS pois ele não era gerado continuamente como recompensa, por isso, esses sempre trocavam seus SLP por AXS acarretando

em um ganho assustadoramente maior para esses indivíduos;

2 - O valor do SLP dependia apenas da necessidade dos breeders de comprar SLP para fazerem novos axies (NFTs), ou seja, o primeiro efeito da entrada massiva de usuários foi o preço do SLP disparar até US\$0,50, porém, uma vez que esses jogadores começaram a ganhar SLP, e vender ele, o preço não parou de cair chegando a US\$0,00196;



Além disso, os NFTs dos personagens não eram realmente únicos e existem dezenas, talvez centenas ou milhares exatamente idênticos conforme foram se descobrindo e configurando os melhores times para se jogar.

E, por isso:

- O jogo passou e passa por muitas reformulações mas sem esperança de jamais o SLP e os axies voltarem no valor que uma boa parte dos usuários pagaram;
- Projetos play-to-earn e NFTs desenvolveram fama de serem maneiras insustentáveis de ganhar dinheiro rápido com modelos econômicos muito similares a de uma pirâmide;

- Se criaram debates extremamente benéficos a respeito de, se os jogos play-to-earn são legítimos por serem focados em ganhar dinheiro e não em se divertir e, também, a respeito de modelos econômicos.
- Se criou, inclusive, um movimento que defende o “re-uso” do modelo “play AND earn” como já foi um dia em jogos como World of Warcraft, onde as pessoas jogavam para se divertir e existia um modelo econômico por conta do valor dos itens na jogabilidade/diversão. A ideia seria utilizar a tecnologia blockchain para tornar esse sistema transparente e muito mais eficiente/transparente, enquanto ele também pode ser de propriedade da própria comunidade.

## AULA 7 - Tokenização

### Como funciona e a ideia da tokenização

A tokenização é uma maneira de usar tokens e contratos inteligentes para digitalizar um modelo de negócios. É uma área que ainda está sendo explorada e não existem receitas.

Por conta das infinitas possibilidades que os smart contracts oferecem, e dos diversos tipos de tokens que existem, que são tanto fungíveis (padrão ERC 20) como não-fungíveis (ERC 721 e ERC 1155), existe muita subjetividade no entendimento dos modelos de tokenização.

É importante que se tenha em mente como se dá o uso dos tokens e smart contracts na digitalização das atividades do modelo proposto bem como entender qual é a interferência humana no funcionamento do mesmo.

Podemos tokenizar um talento de uma pessoa? Depende, como seria feito o procedimento. Se a pessoa é uma cozinheira e ganha dinheiro com o talento ela poderia, quem sabe, levantar fundos para construir seu restaurante e, as pessoas que possuem os tokens, ganharem uma parte do rendimento. Mas o debate seria, o procedimento tokenizou o talento da pessoa ou os

dividendos do restaurante?

**O início e fim de toda atividade tecnológica é o ser humano e por isso sua interação e intervenção deve ser considerada minuciosamente num processo sério de tokenização**

## **Projetos de tokenização fora do comum**

- > **Tokenização de café:** A tokenização de grãos de café em blockchain já existe. O objetivo é criar uma cadeia de abastecimento e rastreio mais eficiente e transparente, permitindo que os compradores verifiquem a origem e a qualidade do café que compram.
- > **Tokenização de ouro:** a tokenização de ouro envolve a criação de tokens que representam a propriedade do ouro físico. Isso permite que os investidores comprem e vendam ouro sem a necessidade de recebimento/entrega ou armazenamento físico do ativo.
- > **Tokenização imobiliária:** envolve a criação de tokens que representam a propriedade de ativos imobiliários. Isso permite que os investidores negoциem frações de propriedades imobiliárias.
- > **Tokenização de arte:** Criação de tokens digitais que representam a propriedade de peças de arte. Isso permite que os investidores comprem e vendam artes digitais e fracionem elas ou até adquiram obras físicas sem a necessidade de custodiar elas.
- > **Tokenização de energia:** Criação de tokens que representam a propriedade de ativos de energia renovável. Isso permite que os investidores comprem e vendam propriedade fracionada em ativos de energia renovável, tornando mais fácil para as pessoas investirem em energia limpa.
- > **Tokenização de músicas:** envolve a criação de tokens digitais que representam a propriedade dos royalties da música. Isso permite que os investidores comprem e vendam propriedade fracionada em royalties de

música, tornando mais fácil para os artistas monetizar sua música.

> **Tokenização de crédito de carbono:** Já existem projetos que usam tanto NFTs como tokens fungíveis e, até um que usa sistemas tecnológicos para medir o impacto real e emitir tokens de acordo com esse impacto.

> **Tokenização de Diamantes:** Funciona através da criação de tanto de NFTs como de tokens fungíveis que representam a propriedade de diamantes físicos.

> **Tokenização de vinho:** Existem casos tanto de coleções/safras bem como de garrafas individuais tokenizadas. Por conta de problemas com autenticidade e a necessidade de criar registros mais confiáveis, a blockchain está sendo [introduzida à indústria](#) do vinho para criar registros imutáveis. Há instâncias tanto do uso de NFTs como de tokens fungíveis para registrar detalhes da origem e processo de manufatura.

## **Collateral/lastro/PEG**

Se fala muito em moeda Fiat/fiduciária. Fiat vem do grego e significa fé. O uso dessa palavra é devido ao valor dessas moedas (real, dólar, euro) estão diretamente relacionados a fé que as instituições que controlam elas.

O mercado cripto, por outro lado, tem várias maneiras de ser medido apesar de algumas métricas como número de holders e volume de negociação poderem ser manipuladas de maneira relativamente fácil. Por isso é importante analisar o que e como pode ser usado como lastro.

> **Gold Standard:** O padrão do ouro regeu a economia americana por um tempo porém foi abandonado. Ele se referia basicamente ao lastro dos dólares circulantes serem colateralizados em ouro. O abandono dessa métrica foi o que permitiu com que o FED imprimisse dinheiro à vontade gerando a desvalorização da moeda. Apenas nos últimos anos aproximadamente 70 a 80% de todos os dólares em circulação foram impressos.

> **Hashrate:** Uma métrica impossível de ser manipulada é a HASHRATE. A hashrate é a quantidade de hashes que estão sendo calculadas por segundo na rede e é, tida por muitos, como um grande lastro do próprio Bitcoin. Inclusive houve uma vez que o Bitcoin foi banido na China, que era responsável por aproximadamente 60% do poder de mineração da rede, resultando em 50% de queda tanto na hashrate como no preço. impressos.

> **Stablecoins:** As principais Stablecoins no dia de hoje são USDT, USDC, BUSD e DAI. Eventualmente temos alguma espécie de auditoria ou interferência qualquer e, uma ou outra, pode perder o lastro/peg. Falência de bancos ameaçam o mercado como um todo, mas já ameaçaram especificamente a moeda USDC que perdeu seu lastro em quase 10%.

## Tipos de NFT (padrões)

> **ERC-721:** ERC-721 é um padrão de token não fungível (NFT) na blockchain Ethereum que permite a criação de ativos digitais exclusivos. Cada token ERC-721 é único e tem seu próprio valor distinto, o que os torna ideais para representar itens raros/colecionáveis, como itens de arte ou jogos ou ativos da vida real como carros, escrituras ou propriedades. O padrão foi amplamente adotado e usado para criar alguns dos NFTs mais populares do mercado atualmente.

> **ERC-1155:** Padrão para criar tokens fungíveis e não-fungíveis na blockchain Ethereum. Ao contrário do padrão ERC-721, que cria tokens exclusivos para cada ativo, o padrão ERC-1155 permite a criação de vários ativos usando um único ativo/contrato inteligente.

> **ERC-998:** ERC-998 é um padrão para criar NFTs complexos na blockchain Ethereum que podem ter várias camadas ou sub-tokens, cada um com suas próprias propriedades e metadados. Isso permite a criação de NFTs mais complexos, como aqueles que contêm vários itens ou têm diferentes níveis de informação/raridade. Alguns veem esse padrão como uma abordagem que possibilita usar a Blockchain de uma maneira mais próxima de um banco

de dados, organizando as informações em “gavetas”. O padrão é projetado para ser compatível com outros padrões ERC, como ERC-721 e ERC-1155, facilitando a integração com projetos existentes.

> **ERC-140**: um padrão proposto para criar NFTs na blockchain Ethereum que estão vinculados a ativos físicos. O padrão é projetado para permitir a criação de NFTs que representam itens físicos, como imóveis, carros ou bens de luxo. Isso tem o potencial de revolucionar a maneira como a propriedade de ativos físicos é registrada e transferida.

> **BEP-721**: padrão de token não fungível (NFT) na Binance Smart Chain (BSC) baseado no padrão Ethereum ERC-721. Ele permite a criação de ativos digitais exclusivos no BSC, que podem ser usados para uma ampla gama de aplicações, incluindo jogos, arte e colecionáveis.

> **TRC-721**: um padrão para criar tokens não fungíveis na blockchain TRON. É semelhante ao padrão ERC-721 na blockchain Ethereum e permite a criação de ativos digitais exclusivos na rede TRON.

> **ERC-721x**: extensão do padrão ERC-721 na blockchain Ethereum que adiciona novos recursos, como transferências em lote, agrupamento de tokens e royalties. Isso facilita o gerenciamento de grandes números de NFTs e permite estratégias de monetização mais avançadas.

> **NEP-11**: NEP-11 é um padrão proposto para criar NFTs na blockchain NEO. É semelhante ao padrão ERC-721 na blockchain Ethereum e permite a criação de ativos digitais exclusivos na rede NEO.

> **NFTS**: Padrão de token não fungível na blockchain Flow, projetado para criar ativos digitais e NFTs. É compatível com os padrões ERC-721 e ERC-1155 da blockchain Ethereum.

> **Tezos FA2**: Tezos FA2 é um padrão para criar tokens fungíveis e não fungíveis na blockchain Tezos. É semelhante ao padrão ERC-1155 na blockchain Ethereum e permite a criação de vários tokens usando um único contrato inteligente.

> **ERC-3475**: um padrão proposto para criar NFTs na blockchain Ethereum que tem vencimento determinado. Inicialmente dentro das mesmas métricas

de títulos e debêntures porém, proporcionam outras possibilidades sem precedentes.

## AULA 8 - Negócios Blockchain, além do Bitcoin - P2P(?), exchanges(CEX/DEX), L2, gateways de pagamento e outros

O Bitcoin representa várias coisas ao mesmo tempo. Além de ser um dinheiro digital ele não possui um gestor/emissor que não seja o código. Diferente de qualquer outro dinheiro do mundo até então.

A mera existência do Bitcoin mudou a compreensão de economistas experientes sobre a inflação por conta de seu limite e curva de emissão (Halving). O que faz com que o Bitcoin seja uma tecnologia que representa, também, uma ideia. A liberdade financeira, ter o poder de “ser seu próprio banco” o que, na prática, se converte em poder participar do sistema financeiro digital do Bitcoin seja tanto usando ele como minerando.

Ele já foi relacionado a crimes e como sendo “um dinheiro de bandidos” porém, ao contrário dos “dólares na cueca”, todas transações ficam registradas para sempre e muitos reguladores que já foram contra ele hoje percebem isso.

Algumas pessoas já perceberam isso antes e começaram a prover serviços para essa esfera de usuários que, apesar de pequena, já possui capitalização de mercado superior a 1 Trilhão de dólares.

## The Bitcoin Standard

As características que fazem do Bitcoin o que é são guias para analisarmos modelos de negócios dentro e fora da indústria. O Modelo de conexão direta (ponto-a-ponto) somado a transparência é uma maneira de fazer negócios interessante que acaba sendo o sucesso do AirBnb por exemplo.

O aplicativo da empresa conecta prestadores e tomadores de serviço e fornece um sistema de avaliação onde a reputação daquele “nó” se dá pela sua atuação na rede. Essas características e algumas outras formam o “padrão Bitcoin” (Bitcoin standard) e é necessário entender e analisar muito bem esses critérios conforme nosso conhecimento expande na indústria para não nos tornarmos parte da “galera do oba-oba cripto”.

Caso não tenha entendido a “galera do oba-oba cripto” são pessoas que estão sempre se empolgando com projetos que possuem modelos econômicos duvidosos e não respeitam os preceito do tal Bitcoin standard e, por consequência, repetidamente caem em golpes ou desistem do mercado ou, às vezes, aplicam golpes por não querer saber a respeito desses preceitos ou até por inocência porém o resultado é sempre o mesmo: pessoas perdendo dinheiro.

Por esse motivo devemos sempre condenar a postura de pessoas que dizem empreender no meio ou criar “conteúdo” e não conhecem/respeitam esses preceitos básicos que devem ser a fundamentação da nossa indústria.

> **Descentralização/distribuição:** Fora a topologia da rede precisamos avaliar a distribuição do poder de mineração (inclusive geograficamente já que, fazendas de mineração), do supply e da tecnologia de mineração já que, eventualmente, alguns projetos surgem com modelos que dependem de máquinas extremamente específicas e inacessíveis.

> **Transparência e anonimidade:** É importante considerar a convergência desses dois conceitos. As transações do Bitcoin podem ser auditadas em tempo real por qualquer pessoa e, ao mesmo tempo, mantém a anonimidade dos participantes pois a única coisa que é revelada é o endereço de carteira.

> **Sem intermediários:** Geralmente a ausência de intermediários vai ser ligada a mediação ser feita pelo código, porém, a centralização, descentralização e distribuição podem ser vistas como estágios de uma organização orgânica, onde uma pessoa ou pequeno grupo tem uma ideia, descentralizam essa iniciativa para outras pessoas com grande autonomia que, por sua vez, distribuem para muitas outras pessoas e capilarizam a operação de maneira natural.

Porém é inegável que a própria Bitcoin School é uma instituição centralizadora e, por um tempo, vamos ter alguns modelos que precisarão desfrutar desse benefício até porque, quando sofremos alguma lesão, por exemplo, quebramos a perna, não queremos uma tomada de decisão distribuída a respeito do que deve ser feito, queremos que um ou mais ORTOPEDISTAS tomem uma decisão baseado nas informações mais modernas possíveis.

> **Responsabilidade financeira:** O limite de emissão controlado pelo código do Bitcoin, a curva de emissão que diminui pela metade a quantidade de Bitcoins emitidos e alguns outros detalhes como os Bitcoins da carteira de Satoshi que jamais foram movimentados deixam claro que o criador do Bitcoin não criou a moeda para seu próprio interesse, não lucrou com a própria criação.

Se Satoshi vender 0,5 BTC da sua carteira provavelmente o mercado vai desabar pois é esse “lucro infinito não realizado” que mantém a confiança das pessoas na responsabilidade financeira do criador, de outra maneira, haveria profundo questionamento dos interesses na criação da principal criptomoeda.

## Exchange, seu banco?

E o que são as exchanges, se não o banco do mercado de criptomoedas? Mesmo com bancos amigáveis a cripto fazendo custódia e provendo liquidez para o mercado as plataformas de negociação popularmente conhecidas como corretoras de criptomoedas ou, preferencialmente, exchanges, são instituições que atuam como os bancos oferecendo custódia dos ativos, programas de rendimento como staking e outros benefícios como a negociação de derivativos.

A realidade é que manter a custódia dos seus ativos e negociar eles diretamente exige certo grau de destreza tecnológica e, além disso, muita responsabilidade dados os inúmeros casos de pessoas que perderam suas chaves privadas.

No “final das contas” as pessoas querem apenas o lado bom das criptomoedas (como de tudo na vida, né?), ou seja, no caso das criptomoedas: o lucro exponencial. E, por esse motivo, os grandes players do mercado acabam vendo grande oportunidade em prestar serviços, serem donos de exchanges.

Nem todas as exchanges operam com transparência e muitas delas são dos mesmos donos e só mudam o software, país sede e “cores do site”. As certificações são as mesmas e, até os funcionários, às vezes são os mesmos.

## DEX x CEX

### > Exchange Centralizada (CEX, Centralized Exchange):

A empresa que gerencia a plataforma atua como intermediário e mantém o controle sobre o processo de negociação e chaves privadas dos usuários.

> Correspondência de Pedidos (Market making): Compradores e vendedores fazem pedidos para comprar ou vender uma criptomoeda ou ativo específico a um determinado preço. O mecanismo de correspondência da exchange combina compradores e vendedores com base em seus critérios de pedido

podendo, inclusive, lucrar com o spread (combinar ordens com valores ligeiramente diferentes e ganhar nessa diferença, spread).

> **Depósitos e saques:** As exchanges fornecem alguma maneira de depositar moedas fiduciárias e sacar elas também conhecidas como fiat on-ramps e off-ramps. O que geralmente ocorre é a plataforma fazer parcerias com instituições locais que provêm liquidez para as transações e repassam as taxas operacionais para os usuários.

Os depósitos podem ser feitos de muitas maneiras, desde cartão de crédito até depósitos ou pix e, da mesma maneira, as retiradas tem critérios mas podem ser, inclusive, via PIX e instantâneas.

> **Taxas de negociação:** É comum pagar taxas de negociação para cada transação, porém, as plataformas com maior volume muitas vezes não cobram taxas pois conseguem lucrar com o market making. As taxas são normalmente uma porcentagem do valor negociado e variam de acordo com o modelo de investimento sendo mais altas em negociações de derivativos, por exemplo.

> **Medidas de segurança:** as CEX geralmente possuem várias medidas de segurança para proteger os fundos e as informações do usuário. Essas medidas podem incluir autenticação multifator, criptografia SSL e armazenamento de parte dos ativos e/ou fundos de garantia em caso de hacks em carteiras frias (offline) `

> **Exchange Descentralizada (DEX, Decentralized exchange):**

Uma DEX é um conjunto de contratos inteligentes que regem/criam uma camada de operação para que usuários possam negociar diretamente sem que uma instituição, como uma CEX, precise fazer a custódia de seus ativos.

> **Sem intermediários:** Apesar de possuírem governança e time de desenvolvimento, as DEX são mediadas por contratos inteligentes, pelo código. Os próprios usuários fazem custódia de seus ativos e os próprios usuários devem atuar como nós da rede. Fazendo esse modelo mais compatível com os fundamentos do BITCOIN STANDARD.

- > **Livro de Pedidos:** O livro de pedidos em uma exchange DEX é descentralizado e mantido no blockchain. Compradores e vendedores fazem pedidos diretamente no blockchain, e esses pedidos são correspondidos automaticamente pelo contrato inteligente.
- > **Pools de liquidez:** as DEX geralmente usam pools de liquidez para garantir que haja uma oferta mais uniforme de ativos para que compradores e vendedores possam negociar com mais fluidez. Essas pools são, em sua grande maioria, fundos cedidos pelos próprios usuários em staking para participar dos ganhos com as taxas.
- > **Custódia:** Em uma DEX, os usuários devem fazer custodia dos seus ativos. Geralmente os usuários usam uma carteira digital como metamask ou trust wallet. Essa carteira é protegida pela chave privada do usuário e o usuário tem controle total sobre seus fundos.
- > **Taxas de negociação:** As taxas de negociação, normalmente, são mais altas do que as cobradas pelas grandes CEX. Além do *slippage* (escorregamento, em tradução livre, variação de preço aceita pelo usuário na compra de um ativo que pode ser necessário ser configurada em até 12%) essas taxas são usadas para incentivar os provedores de liquidez das pools de liquidez.

## Marketplaces

É muito comum ouvir falar de marketplaces NFT, por exemplo, porém até as próprias exchanges podem ser vistas como marketplaces de criptoativos.

- > **Exchanges:** São o tipo mais comum marketplace onde os usuários podem negociar criptomoedas e participar de alguns outros modelos de investimento. Algumas das exchanges mais populares incluem Binance, Coinbase, Kraken, Uniswap, Gate.io e Pancakeswap.
- > **Marketplaces ponto-a-ponto (P2P):** Plataformas que permitem aos usuários comprar e vender criptomoedas diretamente entre si, sem a necessidade de uma troca centralizada. Exemplos de mercados P2P incluem LocalBitcoins, Paxful e Bisq.

- > **Mercados de balcão (OTC, Over the Counter):** Podem ser brokers onde compradores e vendedores podem negociar grandes quantidades de criptomoedas diretamente entre si ou pessoas individuais, OTC traders (erroneamente chamados de P2P no Brasil), que negociam diretamente com o consumidor final. Os mercados OTC são normalmente usados por investidores institucionais e pessoas físicas com alto patrimônio líquido ou pessoas que preferem manter sua privacidade.
- > **Gateways de pagamento em criptomoeda:** Empresas e instituições que prestam serviço fazendo a ponte entre moedas fiduciárias (fiat) e criptomoedas, aceitando ambos. Exemplos de gateways de pagamento incluem BitPay e Coinbase Commerce.
- > **Plataformas de empréstimo de criptomoedas:** são plataformas que permitem aos usuários emprestar ou fazerem empréstimos usando criptomoedas como colateral.
- > **Plataformas de gerenciamento de ativos criptográficos:** são marketplaces que permitem aos usuários investir em um portfólio de criptomoedas, administrado por uma equipe de profissionais. Exemplos de plataformas de gerenciamento de criptoativos incluem Grayscale e Bitwise.
- > **Marketplaces NFT:** são mercados que permitem aos usuários comprar, vender e negociar NFTs que podem ser arte, música ou imóveis virtuais. Alguns mercados NFT populares incluem OpenSea, Rarible e SuperRare.
- > **Marketplaces de arte digital:** são mercados especializados na venda de arte digital, como pinturas digitais, animações e outras criações multimídia. Exemplos de mercados de arte digital incluem Nifty Gateway, Foundation e Async Art.

## **Camada dois (L2, Layer 2)**

As aplicações de segunda camada são uma classe de tecnologias que buscam resolver os problemas de escalabilidade e desempenho associados às redes blockchain. Essas aplicações são construídas em cima de uma blockchain existente, geralmente utilizando contratos inteligentes e outras tecnologias, e permitem que uma grande quantidade de transações seja

processada fora da cadeia principal da blockchain, o que reduz a carga na rede principal e aumenta a capacidade de processamento.

1. **Lightning Network:** Uma camada de pagamento off-chain que permite transações instantâneas e de baixo custo em redes blockchain, como na rede do Bitcoin.
2. **Plasma:** Uma camada de escalabilidade para a Ethereum, que permite que várias "cadeias filhas" sejam executadas em paralelo à cadeia principal.
3. **Raiden Network:** Uma camada de pagamento off-chain para a Ethereum, que permite transações rápidas e escaláveis com taxas mais baixas.
4. **Truebit:** Uma camada de computação fora da cadeia para a Ethereum, que permite que cálculos complexos sejam executados fora da blockchain principal, liberando espaço e recursos para outras transações.
5. **Interledger Protocol:** Uma camada de pagamento inter-blockchain que permite transferências de valor entre diferentes blockchains e redes de pagamento.
6. **Plasma Cash:** Uma variação do Plasma que utiliza tokens não fungíveis em vez de tokens fungíveis para aumentar a escalabilidade e segurança.
7. **OmiseGO:** Uma rede de pagamento descentralizada construída em cima da Ethereum, que permite transferências instantâneas de valor entre diferentes blockchains e sistemas de pagamento.
8. **Matic Network:** Uma camada de escalonamento da rede Ethereum que utiliza uma arquitetura de sidechain para processar transações de maneira rápida.

## Serviços importantes do mercado de criptomoedas

Enquanto alguns se aventuram fazendo e perdendo dinheiro em trades tem algumas empresas/pessoas que estão sempre faturando no mercado.

### > Gateways de pagamento

Gateways de pagamento são serviços on-line que facilitam transações eletrônicas entre clientes e empresas, transmitindo com segurança as informações de pagamento do banco do cliente para o banco do comerciante.

Ele verifica se os fundos estão disponíveis e transfere o valor automaticamente para o comerciante/prestador de serviço.

Esse serviço é essencial no mercado de criptomoedas para que o dinheiro entre e saia do mercado já que todo o sistema é baseado em um sistema de pagamentos digitais.

### > Funcionamento de um gateway de pagamento:

> O cliente inicia uma transação: Ele insere suas informações de pagamento (como detalhes do cartão de crédito) no site ou aplicativo do prestador de serviços.

> O gateway de pagamento recebe a solicitação de transação: transmitindo com segurança as informações de pagamento ao banco do cliente para aprovação.

> O banco do cliente aprova ou recusa a transação: então o banco verifica as informações de pagamento e aprova ou recusa a transação.

> O gateway de pagamento recebe resposta do banco do cliente: mediante a resposta positiva o gateway transfere os fundos automaticamente para o comerciante com as taxas descontadas, caso seja negativa dele avisa que a

transação não foi aprovada.

> O comerciante cumpre o pedido

> Auditorias e consultorias

Toda empresa, eventualmente, precisa ser auditada. As empresas de tecnologia não são diferentes. Possuímos certificados de segurança para contratos de tokens e para muitas outras finalidades.

Além disso, é uma prática comum no meio dos empreendedores ser mentorado ou ter consultoria de alguém com mais experiência no mercado e, por esse motivo, consultorias são um tipo de serviço que “nunca sai de moda”. Por esse motivo o mercado tem tanto empresas como indivíduos que prestam consultoria para todos os tipos de empreendimento web3 em diversas áreas, desde tecnológica, como de estratégia ou marketing e até na área legal.

> Marketing web 3: Agências de Marketing que atendem especificamente empresas de criptomoedas estão se tornando cada vez mais comuns. Elas tendem a ter especialistas de todas as áreas (design, tráfego, videomaker, copywriter) com algum conhecimento em criptomoedas e cargos de gestão/coordenação (planner, manager, BD) geralmente dominados por especialistas e pesquisadores Blockchain além de contarem, muitas vezes, com consultores em tokenização/whitepaper na equipe ou terceiros que prestem esse serviço sob demanda.

> IoT

A difusão da Blockchain está relacionada à confiança gerada pelo código e, em algum momento, para isso acontecer, teremos de ampliar a gama de dispositivos IoT para que todo processo de auditoria, por exemplo, seja automado e “reconhecido tecnologicamente” para ser 100% a prova de falha humana. Por esse motivo se estima que a indústria de IoT vai crescer muito em associação com a expansão de sistemas blockchain mais completos.

> Mineracao, hardware

É uma necessidade da indústria a mineração pois ela mantém as redes funcionando e, por esse motivo, tanto os mineradores como as empresas que vendem as peças específicas (hardware) para essa atividades sempre fazem parte da equação.

O mercado deixa de existir no momento em que as taxas de negociação não conseguirem pagar pela parte técnica de manutenção da rede.

## **O que é liquidez e Marketing Maker**

Liquidez refere-se à eficiência ou facilidade com que um ativo ou título pode ser convertido em dinheiro sem afetar seu preço de mercado.

Um formador de mercado ou provedor de liquidez é uma empresa ou um indivíduo que cota um preço de compra e venda em um ativo negociável no book de ofertas, na esperança de obter lucro com o spread de compra e venda, ou turno.

No módulo 3, veremos mais de perto como ser um provedor de liquidez no mercado descentralizado e gerar renda dessa maneira. Lá, veremos conceitos importantes como: Pool de liquidez, Perda Impermanente, par de liquidez e mais.

## **Potencial Business - seguro de vida, auditoria, monetização de games, gestão de operações complexas**

Hoje existem diversos blockchains com diferentes objetivos específicos. Além disso, também existem aplicativos que utilizam a blockchain para oferecerem soluções únicas e inovadoras. Vamos falar sobre algumas delas.

## > Gala Games

A Gala Games é uma plataforma de jogo play-to-earn baseada em blockchain que recompensa os jogadores com ativos digitais por suas realizações no jogo. São dezenas de games em parceria com diversos estúdios de game.

## > Nexus Mutual

O Nexus Mutual permite que os membros compartilhem riscos. Uma alternativa real de seguro oferecida aos membros. Os especialistas gerenciam o capital agrupado, subscrevem o risco e fornecem cobertura em um mercado de risco globalmente acessível.

## > Certik

A CertiK, também conhecida como Certified Kernel Tech, é uma empresa de segurança web3, blockchain e de contratos inteligentes. A CertiK fornece um Security Leaderboard, uma ferramenta que classifica projetos WEB3 em risco de segurança, com base em uma variedade de primitivas de segurança on-chain.

## > Vechain

Criada em 2015, a VeChain é uma plataforma blockchain com a missão de simplificar o gerenciamento da cadeia de suprimentos com tecnologia de contabilidade distribuída (DIT). O VeChain foi projetado para melhorar o fluxo das cadeias de suprimentos e aprimorar os processos de negócios com a ajuda da tecnologia de contabilidade distribuída segura.

## > Looks Rare

Looks Rare é um mercado da comunidade para negociar NFTs e colecionáveis digitais no Ethereum. O principal marketplace de NFTs do mercado é o Open Sea, uma das plataformas mais lucrativas do mercado de criptomoedas.

## História do crash da FTX

A exchange de criptomoedas FTX e seu fundador e ex-CEO, Sam Bankman-Fried, estão intimamente ligados. O colapso rápido e prejudicial da FTX no final de 2022 teve repercussões na comunidade criptográfica internacional.



O colapso da FTX ocorreu em cerca de 10 dias em novembro de 2022. O catalisador foi um furo de reportagem de 2 de novembro do site de notícias cripto CoinDesk, que revelou que a Alameda Research, a empresa de negociação quantitativa também administrada por Bankman-Fried, detinha uma posição avaliada em US\$ 5 bilhões em FTT, o token nativo do FTX.

O relatório revelou que a base de investimento da Alameda também estava no FTT, o token que sua empresa irmã havia inventado, não em uma moeda fiduciária ou outra criptomoeda.

Isso gerou preocupação em todo o setor de criptomoedas em relação à alavancagem e solvência (Solvência, em finanças e contabilidade, é o estado do devedor que possui seu ativo maior do que o passivo, ou a sua

capacidade de cumprir os compromissos com os recursos que constituem seu patrimônio ou seu ativo.) não reveladas das empresas de Bankman-Fried.

Uma sequência de eventos ocorrem que contribuíram para a derrocada da corretora FTX.

**6 de novembro:** A exchange rival Binance vende todos os tokens FTT.

> **7 de novembro:** FTX anuncia crise de liquidez, busca resgate de capitalistas de risco e depois da Binance.

> **8 de novembro:** Binance diz que comprará os negócios fora dos EUA da FTX.

> **9 de novembro:** Binance se afasta da aquisição da FTX após conduzir a devida diligência.

> **10 de novembro:** Bahamas congelam os ativos da subsidiária da FTX lá; Bankman-Fried admite crise de liquidez de empresas fora dos EUA, diz que a afiliada Alameda Research vai diminuir.

> **11 de novembro:** Bankman-Fried deixa o cargo de CEO da FTX e é substituído por um CEO nomeado pelo tribunal com experiência em reestruturação.

> **12 de novembro:** FTX relata um suposto hack, suspeito de ser de até \$477 milhões, e move seus ativos digitais para armazenamento frio por motivos de segurança.

> **18 de novembro:** Bahamas assume o controle dos ativos da FTX ali mantidos.

> **12 de dezembro:** Bankman-Fried é preso pelas autoridades das Bahamas. Mais tarde, ele é extraditado para os EUA.

> **22 de dezembro:** Bankman-Fried é libertado sob fiança de US\$250 milhões, a maior da história, por um juiz federal.

> Segundo as últimas notícias, cerca de 1 Bilhão de dólares foram perdidos na quebra da FTX. O ocorrido afetou fortemente a credibilidade do mercado de criptomoedas, gerando ainda mais medo e desinformação na população.

## AULA 9 BLOCKCHAIN para nerds vol 1

### Por que Blockchain para nerds?

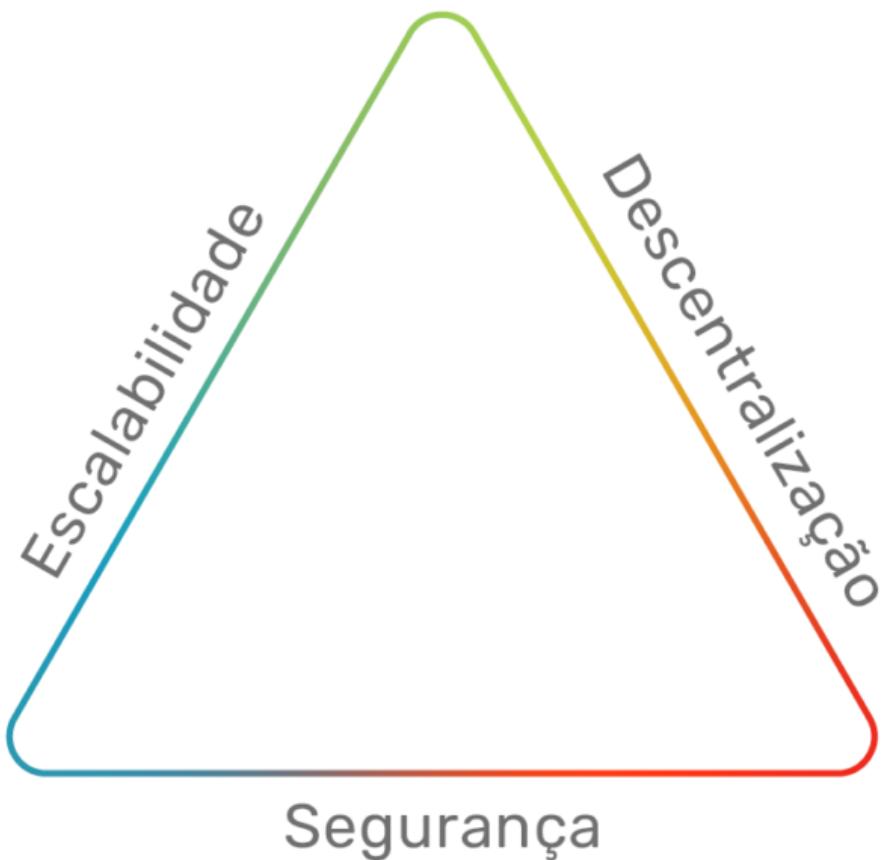
Existem conceitos sobre blockchain que, apesar de serem desconhecidos pela grande maioria, podem trazer grande diferencial na elaboração de projetos, conhecimento da cultura e na análise de projetos.

No blockchain para nerds, você vai entender conceitos técnicos de forma simplificada e conhecer as principais ferramentas utilizadas por insiders do mercado.

Alguns conceitos podem e devem evoluir com o desenvolvimento das tecnologias atuais e das novas tecnologias. Mas Core (o núcleo) do conhecimento permanece.

### O que é o trilema blockchain?

O trilema blockchain é uma teoria que afirma que é impossível para uma rede blockchain ser simultaneamente segura, descentralizada e escalável. Esses três elementos são considerados essenciais para uma rede blockchain bem-sucedida, mas são difíceis de serem alcançados em conjunto.



Segurança refere-se à capacidade da rede de resistir a ataques maliciosos e garantir que as transações sejam autênticas e válidas. Descentralização é a capacidade da rede de ser distribuída entre vários nós de rede independentes, em vez de depender de uma única autoridade central. A escalabilidade é a capacidade da rede de processar um grande número de transações de maneira eficiente e sem comprometer a segurança ou a descentralização.

O trilema blockchain argumenta que, embora seja possível ter duas dessas características em conjunto, é impossível ter todas elas. Por exemplo, se uma rede blockchain for altamente descentralizada e segura, é provável que ela tenha dificuldades para escalar e lidar com um grande número de transações. Da mesma forma, se uma rede blockchain for altamente escalável e segura, é provável que ela seja centralizada e, portanto, perca sua natureza descentralizada.

Esta teoria é frequentemente citada para explicar por que muitas redes blockchain ainda lutam para atingir todos os três elementos de maneira satisfatória. À medida que a tecnologia blockchain continua a evoluir, os desenvolvedores estão trabalhando para encontrar soluções que equilibrem esses três elementos e permitam que as redes blockchain funcionem de maneira eficiente e segura em uma variedade de cenários.

## Análise do trilema em algumas moedas

A análise em relação ao trilema pode levar em consideração diferentes pontos de vista. Vamos analisar algumas das principais blockchains.

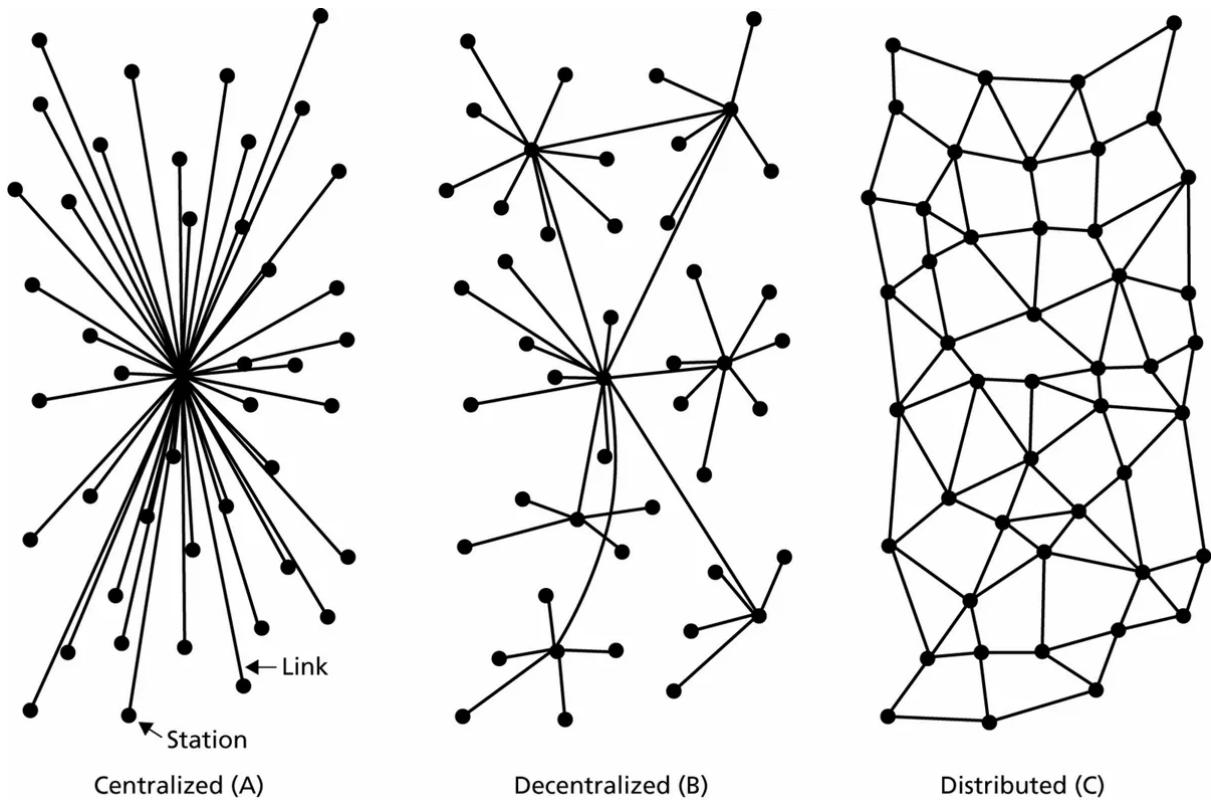
**Ethereum >** Considerada uma das blockchains mais seguras da atualidade, ela possui um nível de descentralização razoável em consideração a maioria das blockchains, porém possui um grande problema quanto a escalabilidade.

**Solana >** Ao contrário da Ethereum, a blockchain solana é altamente escalável com transações rápidas, possui um nível de descentralização razoável com mais de 1500 nós validadores espalhados pela rede e seu ponto fraco está na segurança da rede.

**BNB Chain >** É uma blockchain desenvolvida pela corretora Binance e que possui alta escalabilidade e segurança, porém é uma rede altamente centralizada. Visto que para garantir a segurança da rede, a rede possui cerca de 41 validadores até o presente momento.

## Centralizado, descentralizado, distribuído

Vimos um pouco sobre esses conceito na aula 3 em "Como funciona a blockchain", agora vamos entender melhor de forma técnica a imagem abaixo.



Centralizado, descentralizado e distribuído são termos que descrevem diferentes formas de organização e controle de sistemas ou redes. Cada um desses termos tem implicações diferentes para a segurança, eficiência e resiliência do sistema.

**Centralizado:** um sistema centralizado é aquele em que todo o controle e tomada de decisões é realizado por uma única entidade central. Nesse modelo, todos os dados e decisões fluem para e a partir de uma única fonte, e a tomada de decisões é realizada por uma única autoridade. Isso pode ser eficiente em alguns casos, mas pode deixar o sistema vulnerável a falhas, já que todos os dados estão centralizados em um só lugar.

**Descentralizado:** um sistema descentralizado é aquele em que o controle e a tomada de decisões são distribuídos entre várias entidades independentes. Nesse modelo, várias autoridades independentes trabalham juntas para tomar decisões e gerenciar o sistema. Isso pode tornar o sistema mais resiliente e menos vulnerável a falhas, mas pode ser menos eficiente em alguns casos, já que a tomada de decisões pode ser mais demorada devido à necessidade de coordenação.

Distribuído: um sistema distribuído é aquele em que o controle e a tomada de decisões são compartilhados entre várias entidades independentes, com cada entidade tendo acesso a todos os dados. Nesse modelo, cada entidade pode tomar decisões independentes e pode trabalhar em paralelo para processar dados e realizar tarefas. Isso pode tornar o sistema altamente eficiente e resiliente, já que as entidades podem continuar a operar mesmo se uma parte do sistema falhar. No entanto, pode ser mais complexo de configurar e gerenciar.

Em resumo, um sistema centralizado tem controle e tomada de decisões centralizados em uma única autoridade, um sistema descentralizado tem várias autoridades independentes que trabalham juntas para tomar decisões e um sistema distribuído tem várias autoridades independentes que compartilham o controle e a tomada de decisões. Cada modelo tem vantagens e desvantagens, e a escolha do modelo mais adequado depende das necessidades e objetivos específicos do sistema.

## **Importância da distribuição do poder econômico motivo do bitcoin existir**

A distribuição do poder econômico é extremamente importante em qualquer sociedade. Quando a riqueza é concentrada nas mãos de poucos indivíduos ou empresas, pode haver uma série de efeitos negativos, como aumento da desigualdade social, falta de oportunidades para indivíduos e empresas menores e aumento da instabilidade econômica.

O Bitcoin surgiu como uma resposta a essa concentração de poder econômico. A moeda digital foi criada como uma alternativa descentralizada e independente do sistema financeiro tradicional, em que o poder econômico é concentrado em grandes bancos e instituições financeiras. Ao contrário das moedas tradicionais, o Bitcoin não é controlado por um único órgão ou instituição financeira. Em vez disso, ele é mantido por uma rede descentralizada de usuários e mineradores que validam as transações e mantêm a segurança da rede. Isso significa que o poder econômico não é concentrado em uma única entidade, mas distribuído entre os usuários da rede.

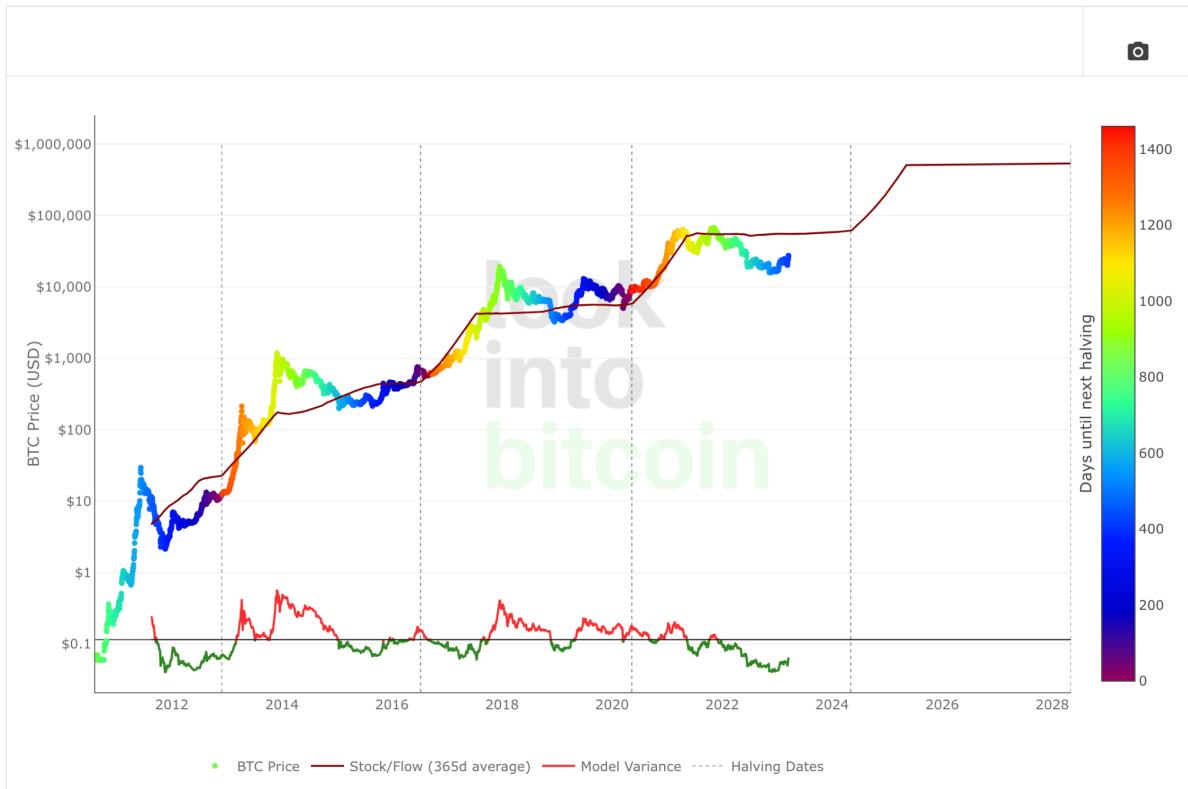
É importante destacar que, mesmo na rede do Bitcoin, existe certa centralização de cursos, o que abre margens para uma grande discussão. Contudo, o Bitcoin continua sendo ferramenta fundamental para distribuição de recursos.

A distribuição descentralizada do poder econômico é uma das principais razões pelas quais o Bitcoin é tão atraente para muitas pessoas. Ele permite que indivíduos e empresas de todos os tamanhos participem da economia global de forma mais justa e equitativa, sem depender de grandes instituições financeiras ou governos.

Em resumo, a importância da distribuição do poder econômico é fundamental para garantir uma economia mais justa e equitativa para todos os participantes. O Bitcoin existe como uma resposta a essa necessidade, proporcionando uma alternativa descentralizada e independente para o sistema financeiro tradicional.

## **Modelo stock-2-flow**

O modelo Stock-to-Flow é um modelo econômico que tem sido usado para avaliar a escassez de recursos e produtos em um mercado. O modelo mede a quantidade de um determinado recurso ou produto existente em relação à quantidade produzida anualmente (fluxo). Essa relação é chamada de "Stock-to-Flow ratio" (relação estoque-fluxo, em tradução livre).



O modelo tem sido aplicado com frequência no mercado de criptomoedas, particularmente com relação ao Bitcoin. Nesse contexto, o modelo mede a quantidade de Bitcoins existentes em relação à quantidade produzida anualmente, que é limitada pelo algoritmo da criptomoeda. Essa relação é usada para prever o preço futuro do Bitcoin, já que o modelo sugere que quanto maior a relação Stock-to-Flow, maior será o valor da criptomoeda.

Um dos principais mecanismos é o Halving. O Halving no Bitcoin é um evento programado que ocorre aproximadamente a cada 4 anos (ou 210 mil blocos), onde a recompensa que os mineradores de Bitcoin recebem é cortada pela metade. Isso significa que a quantidade de novos Bitcoins que são criados a cada bloco minerado é reduzida pela metade. Essa emissão continua até o limite de 21 milhões de moedas mineradas.

## Ferramentas de análise on-chain

As blockchains em geral podem ser privadas, públicas ou híbridas. As blockchains públicas permitem que qualquer pessoa faça auditoria dos

códigos e saiba o que está acontecendo em tempo real. Isso abre margem para utilização de ferramentas que rastreiam as movimentações dentro da blockchain (on-chain).

#### > [Whale alert](#)

Whale Alert é um serviço de notificação de grandes movimentos de capital das baleias no mercado criptográfico. Ele permite que você receba notificações instantâneas assim que houver uma grande movimentação de tokens na rede blockchain. Assim, toda vez que o detentor de grande valores movimenta dinheiro, recebemos essa informação, que é pública. Uma das principais fontes de informações do mercado é o Twitter.

#### > [Dune](#)

Dune Analytics é um provedor de dados de código aberto baseado na comunidade que permite a qualquer pessoa publicar e acessar tendências de criptografia em tempo real. Fundada por Fredrik Haga e Mats Olsen em 2018, a Dune Analytics é uma plataforma de análise baseada em Ethereum que torna os dados criptográficos on-chain acessíveis e consumíveis. Uma das melhores ferramentas de análises do mercado. Podemos analisar a movimentação em corretoras, marketplaces, fazer comparações entre elas e muito mais.

#### > [DeBank](#)

DeBank é um painel para rastrear seu portfólio DeFi (Finanças Descentralizadas), com dados e análises para protocolos de empréstimos descentralizados, stablecoins, plataformas de negociação de margem e DEXes.

#### > [Apeboard](#)

O Ape Board é um painel DeFi cross-chain (funciona em diversas redes blockchain) - semelhante ao Zerion e Zapper - onde você pode monitorar os saldos de seu portfólio ou de outras pessoas nos protocolos DeFi.

## > Glassnode

Glassnode traz inteligência de dados para o espaço blockchain e criptomoeda. A Glassnode cria aplicativos que fornecem novas maneiras de fornecer insights sobre blockchains e criptomoedas, concentrando-se na fonte de entrada mais importante no espaço: dados dos próprios blockchains. Os dados gerados pela Glassnode são utilizados por grandes analistas e traders do mercado.

## > Nansen

Nansen é uma plataforma de análise de blockchain que enriquece os dados on-chain com milhões de análises. Os investidores usam o Nansen para descobrir oportunidades, realizar due diligence e defender seus portfólios com os painéis e alertas em tempo real. É uma das ferramentas mais utilizadas no mercado NFT.

## > Token Terminal

O Token Terminal é uma plataforma que agrupa dados financeiros nas principais blockchains e aplicativos descentralizados. É similar a outras ferramentas de análise como a Glassnode.

## > Messari

A Messari fornece inteligência de mercado confiável para investidores e profissionais de criptomoedas, para que possam tomar melhores decisões. É uma das principais ferramentas de análise do mercado, além de possuir um grande acervo de conteúdos.

## **RPC - Remote Procedure Call**

Uma chamada de procedimento remoto ou nó RPC é um tipo de servidor de computador que permite aos usuários ler dados no blockchain e enviar transações para diferentes redes. Como por padrão acessamos um nó na rede para ter acesso a blockchain, podemos adicionar uma rede de forma manual da seguinte forma na Metamask:

## Redes > Adicionar uma rede > Add a network manually

---



Um provedor de rede mal-intencionado pode mentir sobre o estado do blockchain e registrar as atividades da sua rede. Adicione somente as redes personalizadas em que você confia.

### Nome da rede

### Novo URL da RPC

### ID da cadeia

### Símbolo da moeda

### URL do Block Explorer (Opcional)

[Cancelar](#)[Salvar](#)

## UTXO - Unspent Transaction Output

Uma saída de transação não gasta (UTXO) é o termo técnico para a quantidade de moeda digital que permanece após uma transação de criptomoeda. Você pode pensar nisso como o troco que recebe depois de comprar um item, mas não é uma denominação mais baixa da moeda - é uma saída de transação no banco de dados gerada pela rede para permitir

transações de troco não exatas. É dessa forma que as transações acontecem na rede Bitcoin.

## MEMPOOL

A mempool é a área de espera de criptomoedas para transações não confirmadas que aguardam ser capturadas pelos mineradores.

De um modo geral, um mempool é uma fila organizada onde as transações são armazenadas e classificadas antes de serem adicionadas a um bloco recém-criado. O pool de memória contém transações “frescas” ou não confirmadas (armazenadas como transações individuais). A blockchain contém transações “arquivadas” ou confirmadas (empacotadas em “blocos”).

# AULA 10 BLOCKCHAIN para nerds vol 2

## Layers

Nesse momento, provavelmente você já ouviu falar sobre soluções layer 2 ou soluções de segunda camada. Assim como na internet possuímos uma arquitetura para trabalhar cada função de forma separada, na blockchain também temos diferentes camadas.

Veja o exemplo dos modelos OSI e TCP/IP. Os padrões de arquitetura mais utilizados na internet.



Modelo de Referência OSI



Modelo TCP/IP

Agora, na arquitetura blockchain possuímos as camadas: 0, 1, 2 e 3. Assim como na internet, existem diferentes modelos e interpretações, então vamos utilizar o modelo mais aceito e utilizado na área.



Vamos ao fundamento de cada camada.

> Camada 0

A camada mais baixa. Consiste no hardware, internet e conexões que permitiriam que os blockchains da Camada 1 funcionem de maneira suave e eficiente. Protocolos a partir dos quais blockchains inteiros podem ser construídos e permitem a interoperabilidade entre essas cadeias também estão nessa camada.

Um protocolo popular nesta camada é o Cosmos. O Cosmos fornece ferramentas de código aberto que permitem que os blockchains construídos com eles sejam interoperáveis e se comuniquem entre si, enquanto ainda permite que os projetos atendam às suas próprias necessidades de blockchain. Por causa disso, os custos de gás podem ser reduzidos sem afetar muito o rendimento.

#### > Camada 1

A própria blockchain é a camada responsável pela segurança. Essa camada garante que os protocolos da rede blockchain sejam seguidos e implementados. Ele realiza os processos de consenso, linguagens de programação e outros processos técnicos para finalizar as transações em sua cadeia. Em suma, geralmente se preocupa com a criação e adição de novos blocos à cadeia.

Os amplamente conhecidos Bitcoin e Ethereum são exemplos de blockchains L1.

#### > Camada 2

Essa camada se concentra na escalabilidade e é onde os aplicativos são executados. Ele atua como uma integração de terceiros que lida principalmente com todas as autenticações de transação, sendo construído sobre o L1 e se comunicando continuamente com ele. Isso permite que mais nós sejam adicionados à rede, o que aumenta a taxa de transferência sem obstruir muito o L1.

Polygon é um exemplo de uma rede de Camada 2 construída para ajudar a dimensionar o blockchain Ethereum. Ele é executado ao lado do Ethereum, agrupando várias transações em uma e postando-as de volta no L1. Ele permite transações mais rápidas, o que acaba reduzindo as taxas de gás.

#### > Camada 3

L3 é a interface do usuário que fala com o blockchain e os usuários finais. Os aplicativos criados nessa camada permitem usos do mundo real do blockchain, como jogos, finanças descentralizadas (DeFi) e armazenamento.

Muitos desses aplicativos também possuem recursos de cadeia cruzada que permitem que usuários de vários blockchains os usem

Um exemplo de uso de camada 3 é o Uniswap, que é uma troca de criptografia baseada em Ethereum automatizada e descentralizada. O aplicativo descentralizado (DApp) permite que os usuários negoçiem suas criptomoedas com taxas mais baixas, em oposição às trocas centralizadas de books de ofertas, como Binance e Coinbase. Também não exige que os usuários desistam de suas chaves privadas, o que torna a negociação mais segura.

À medida que as pessoas começam a usar amplamente blockchain e criptomoedas, ainda há muito a melhorar com seu desenvolvimento. Como resultado, essas camadas podem encontrar problemas de tempos em tempos, mas devido à crescente adoção da criptografia e aos casos de uso que o blockchain traz, muitas empresas e indivíduos estão constantemente trabalhando para tornar as camadas de blockchain mais seguras, escaláveis e descentralizadas.

## ZK - Zero-Knowledge Prove

Uma prova de conhecimento zero é uma maneira de provar a validade de uma afirmação sem revelar a afirmação em si. O 'validador' é a parte que tenta provar uma reivindicação, enquanto o 'verificador' é responsável por validar a reivindicação.

As provas de conhecimento zero apareceram pela primeira vez em um artigo de 1985, "A complexidade do conhecimento dos sistemas de prova interativos", que fornece uma definição de provas de conhecimento zero amplamente usadas hoje:

Um protocolo de conhecimento zero é um método pelo qual uma parte (o validador) pode provar à outra parte (o verificador) que algo é verdadeiro, sem revelar nenhuma informação além do fato de que essa afirmação específica é verdadeira.

As provas de conhecimento zero melhoraram ao longo dos anos e agora estão sendo usadas em várias aplicações do mundo real.

A tecnologia está em constante evolução e existe certa complexidade em seus conceitos técnicos. Caso queira entender melhor seu funcionamentos, acesse: <https://ethereum.org/pt/zero-knowledge-proofs/>

## O que são Derivativos

Derivativos são instrumentos financeiros cujos valores e preços são derivados de outro ativo subjacente, como ações, commodities, moedas, índices de mercado, taxas de juros e outros ativos financeiros. Eles são usados para gerenciar riscos e especular sobre movimentos futuros de preços de ativos subjacentes.

### > Ativos sintéticos

Um exemplo de derivativo são os ativos sintéticos que são muito comuns dentro do mercado de criptomoedas. Ativos como WBTC, WETH, WSOL são derivativos dos tokens principais.

Mas por que precisamos de ativos que imitam os ativos reais?

A Blockchain do Bitcoin foi construída de forma diferente da Ethereum, por exemplo, e o padrão programado para o Bitcoin, não se comunica com a rede Ethereum. Para tornar o Bitcoin negociável dentro da rede Ethereum, um sintético de Bitcoin chamado WBTC foi criado para ser negociado dentro da rede Ethereum e nos protocolos de finanças descentralizadas.

Isso permite com que existam mais Bitcoins do que deveria? Não exatamente, para controlar a quantidade de sintéticos nas diferentes blockchains, utilizamos um mecanismo chamado de Bridge ou "ponte" na tradução literal.

## Como funciona day trade

Os derivativos permitem a utilização do mercado futuro, em que você consegue negociar uma representação do ativo real. Se comprarmos um derivativo de Bitcoin no mercado futuro, isso significa que eu não tenho o Bitcoin, mas uma representação dele, um "papel" de Bitcoin.

Esse mecanismo permite com que Traders operem vendido no mercado, ou seja, apostando na baixa do ativo. Além disso, é possível utilizar alavancagem no mercado, o que significa que o usuário pode comprar mais do que tem de capital em conta. Contudo é importante destacar que a alavancagem possui grande risco associado, aumentando a possibilidade de ganhos e também aumentando a possibilidade de perda.

É muito comum os grandes players manipularem o mercado para liquidar a maioria dos traders. Isso significa que o preço é levado além do limite de margem dos traders. Fazendo com que os traders percam todo dinheiro na carteira futuros.

## O que são Bridges

Os investidores estão gradualmente demonstrando mais interesse no campo de DeFi. Portanto, os usos de uma ponte blockchain estão gradualmente ganhando força no ecossistema de aplicativos descentralizados.

Assim como as pontes físicas, a ponte blockchain conecta duas redes ou aplicativos blockchain separados. Uma ponte blockchain pode funcionar de maneiras diferentes e também é chamada de 'ponte entre cadeias'. Ele pode facilitar a transferência ininterrupta de ativos e informações entre redes de camada 1 e camada 2, bem como entre diferentes redes de blockchain.

Cada projeto blockchain apresenta parâmetros de definição específicos exclusivos para o projeto, que criam problemas de interoperabilidade. Uma ponte blockchain serve como a resposta comprovada para esse problema, pois pode servir como modos sem confiança, confiáveis, bidirecionais ou unidirecionais para transferir diferentes transações e conjuntos de dados por

meio de pontes blockchain. O funcionamento de uma ponte blockchain pode envolver a troca de identidades descentralizadas, informações fora da cadeia e chamadas de contratos inteligentes.

Quando utilizamos sintéticos, utilizamos uma cópia de um ativo real, que normalmente está "preso" em uma ponte (contrato inteligente). É importante ressaltar que existem riscos associados aos contratos inteligentes de pontes. Utilizar ativos sintéticos gera uma camada maior de risco para os usuários.

## **EVM - Ethereum Virtual Machine**

A Máquina Virtual Ethereum ou EVM é um software que executa contratos inteligentes e calcula o estado da rede Ethereum após cada novo bloco ser adicionado à cadeia. O EVM fica no topo do hardware da Ethereum e da camada de rede de nós.

Algumas Blockchains foram criadas de forma a serem compatíveis com a Máquina Virtual da Ethereum, o que explica por que precisamos de diferentes carteiras dependendo da blockchain que estamos acessando.

Quando utilizando a Meta Mask, por exemplo, podemos acessar diferentes blockchains, como: Avalanche, Polygon, Arbitrum, Fantom, BNB chain, entre outros. Porém, algumas blockchains não podem ser acessadas pela Meta Mask por falta de compatibilidade com a EVM. Isso significa que blockchains como a Polkadot, Tezos e outras, não são EVM compatíveis, e precisam de uma carteira própria de acesso.

# AULA 11 BLOCKCHAIN para nerds

## vol 3

### Defi, Gamefi, e outras trends

O mercado de criptomoedas segue por diferentes narrativas, aqui vamos ver algumas das principais narrativas do mercado.

#### > Defi

Os mecanismos de finanças descentralizadas ganharam grande força nos últimos ciclos de alta do mercado, através desse mecanismo conseguimos ter acesso a diversas soluções financeiras, como tomar empréstimos, seguros e receita em ativos emprestados.

Existem muitos profissionais especializados nessas soluções financeiras. São infinitas soluções e possibilidades de investimento. Diversas narrativas já surgiram dentro deste segmento, como, por exemplo, os super Yields.

#### > Super Yields

Super Yields ou Mega Yields, foi uma narrativa que oferecia Staking (uma forma de investimento) com um rendimento anual de 10 mil% ou mais. Pois é, loucura! Surgiram centenas de novos projetos oferecendo receitas absurdas. E nesse momento as pessoas começaram a questionar a sustentabilidade desses retornos. A resposta era óbvia! Não existe almoço grátis. A maioria dos projetos ou morreu, ou diminuiu drasticamente os retornos. Isso porque os rendimentos pagos eram pagos em token próprio por meio de emissão, gerando assim uma grande inflação no token.

A conta é bem simples. Preço do token = Capitalização de mercado / Quantidade de moedas.

Isso significa que a quantidade de moedas é inversamente proporcional ao preço do ativo. Logo, se aumentamos o número de moedas no mercado, diminuímos o preço do ativo.

É importante ressaltar que existem mecanismos como o de queima de tokens, utilizado para equilibrar a balança e manter o preço do ativo.

#### > Real Yield

A quebra de grandes tokens que utilizavam o super yield abriu margem para outra narrativa! O Real Yield. Como o nome já sugere, trata-se de uma receita sobre um lucro real, sem emissão de tokens desenfreada.

A corretora descentralizada GMX ganhou muita atenção por utilizar um mecanismo de receita sobre lucros reais. Os investidores emprestam o dinheiro para os traders trabalharem, como a maioria perde o dinheiro nas operações, esses são distribuídos de acordo com o dinheiro investido por cada usuário.

Existem diversos projetos e tokens dentro dessa narrativa que a cada dia ganha mais atenção no mercado. Mas essa não foi a única ferramenta utilizada pela GMX. Conhecer a Teoria dos jogos é fundamental para entender mais a fundo os mecanismos de Finanças Descentralizadas.

#### > Gamefi

GameFi é uma tendência na indústria de jogos que combina elementos de jogos e finanças descentralizadas (DeFi). A GameFi permite aos jogadores ganhar recompensas em criptomoedas por meio da participação em jogos, tornando o jogo uma forma de investimento financeiro.

Os jogadores podem ganhar criptomoedas, tokens não fungíveis (NFTs) e outros ativos digitais ao completar tarefas em jogos ou ao atingir determinados marcos. Além disso, os jogadores podem comprar, vender ou trocar esses ativos em mercados de criptomoedas descentralizados.

Um grande exemplo é o game Axie Infinity, que influenciou milhares de pessoas no mundo. Contudo, a economia do game mostrou-se insustentável, assim como a maioria dos games relacionados a finanças descentralizadas.

Apesar de possuírem poucos exemplos de sucesso na narrativa, ainda estamos em um processo embrionário. O que significa que os modelos Play-to-Earn (jogue para ganhar) ainda vão evoluir bastante nos próximos anos.

#### > Liquid Staking

Liquid staking, também conhecido como soft staking, é uma forma mais avançada de staking tradicional que está disponível em muitos protocolos de contratos inteligentes de nova geração. Com os Stakings líquidos, os usuários podem acessar seus fundos bloqueados para outras atividades baseadas em criptografia enquanto ainda ganham recompensas de seu depósito original.

A Lido finance é um grande exemplo disso! Quando colocamos o token ETH em staking (travado) para receber uma recompensa mensal dentro do protocolo, recebemos um derivativo chamado stETH para utilizar em outros locais. Gerando infinitas possibilidades com o derivativo. Algo que chamamos de Money Legos ou Yield Hacking.

#### > ReFi

#### > SocialFi

## **Yield hacking**

Yield hacking é uma estratégia financeira que busca maximizar os rendimentos ou retornos financeiros de um investimento utilizando diversas técnicas e ferramentas disponíveis no mercado. Essa estratégia é aplicada em investimentos em finanças descentralizadas (DeFi). O yield hacking envolve a utilização de várias técnicas, como a realização de arbitragem, o fornecimento de liquidez em pools de liquidez em exchanges descentralizadas (DEX), a participação em programas de recompensa e a negociação de tokens de governança, entre outras.

A arbitragem, por exemplo, envolve a compra e venda de um ativo em diferentes exchanges para aproveitar as diferenças de preços. Já o fornecimento de liquidez em pools de liquidez em exchanges descentralizadas envolve a disponibilização de um ativo para ser usado em trocas, recebendo uma taxa de juros em troca.

O yield hacking é considerado uma técnica avançada de investimento e requer um conhecimento aprofundado dos mercados financeiros, bem como a capacidade de identificar oportunidades de investimento com alto potencial de retorno. No entanto, é importante ressaltar que, assim como qualquer investimento, o yield hacking envolve riscos e pode resultar em perdas.

## Teoria dos Jogos

A teoria dos jogos é uma área da matemática aplicada que estuda o comportamento estratégico de indivíduos ou organizações em situações de tomada de decisão, chamadas de "jogos". A teoria dos jogos é frequentemente usada em economia, ciência política, psicologia, sociologia e outras disciplinas que envolvem a análise de comportamentos estratégicos.

Os "jogos" na teoria dos jogos não se limitam a jogos de tabuleiro ou videogames, mas sim a qualquer situação em que indivíduos ou organizações tomam decisões que afetam uns aos outros. Um exemplo comum de jogo é o dilema do prisioneiro, em que dois criminosos são presos e interrogados individualmente. Cada um tem a opção de confessar ou não confessar, e suas sentenças dependem das escolhas que fazem e das escolhas feitas pelo outro. Se os dois não confessarem, todos saem ganhando. Através dessas teorias e estudos estratégias são criadas em Defi para manter os investidores em um mesmo projeto.



A teoria dos jogos ajuda a modelar e prever o comportamento de indivíduos e organizações em situações de tomada de decisão complexas. Ela pode ser usada para analisar o comportamento de empresas em um mercado competitivo, ou para entender a dinâmica de conflitos entre países. A teoria dos jogos também é utilizada em estratégias de negociação, marketing e tomada de decisões em geral.

## AirDrop

Airdrop é uma forma de distribuição de criptomoedas ou tokens digitais gratuitamente para um grande número de pessoas. Na prática, o airdrop funciona como uma campanha de marketing para promover uma nova criptomoeda ou um projeto blockchain, atraindo a atenção de mais usuários.

Durante um airdrop, os usuários precisam cumprir certos requisitos, como seguir uma conta nas redes sociais, participar de grupos de , utilizar determinado aplicativo ou baixar um aplicativo específico. Uma vez que os requisitos sejam atendidos, os usuários recebem uma quantidade predeterminada de criptomoedas ou tokens digitais.

Os airdrops podem ser realizados para promover uma nova criptomoeda, uma oferta inicial de moedas (ICO) ou para distribuir tokens de governança em projetos blockchain existentes. Eles podem ser uma estratégia eficaz para

aumentar a visibilidade de um projeto blockchain e atrair novos usuários e investidores.

No entanto, é importante notar que nem todos os airdrops são legítimos e alguns podem ser usados como um meio de golpe ou fraude. É importante pesquisar cuidadosamente antes de participar de um airdrop e garantir que a criptomoeda ou token distribuído tenha um valor real e seja apoiado por um projeto sólido.

## O que é ESG

ESG significa Environmental(Ambiental), Social e Governança(Governança), e é uma estratégia de longo prazo empregada por empresas que se preocupam com o impacto que suas atividades tem no mundo.

É uma área que ainda flutua no radar dos investidores que, eventualmente, usam as práticas ESG como métricas para avaliar a sustentabilidade e o impacto ético de seus investimentos. O ESG tornou-se mais relevante nos últimos anos, à medida que os investidores se tornaram mais conscientes do impacto que seus investimentos têm no mundo ao seu redor.

Como a Blockchain é uma tecnologia auditável, transparente e que cria registros imutáveis ela pode desempenhar um papel importante na promoção e avanço dos princípios ESG.

Fornecendo transparência e rastreabilidade aos investimentos ESG, a blockchain permite que os investidores possam acompanhar as atividades da instituição, garantindo que estejam indo para projetos sustentáveis e éticos. Além disso, o blockchain pode fornecer dados sobre o impacto ambiental dos investimentos, como emissões de carbono ou uso de água.

E, mais que isso, as criptomoedas podem permitir maior acesso para investir e iniciar projetos ESG. Ao investir em criptoativos vinculados a projetos ESG, os investidores podem apoiar iniciativas sustentáveis e éticas diretamente, sem passar por intermediários financeiros tradicionais e instituições que podem estar fazendo “green washing”. Isso pode ajudar a contornar intermediários que podem não ter o mesmo comprometimento com os

princípios ESG, levando a um impacto mais direto e efetivo no meio ambiente e na sociedade.

É possível usar o sistema Blockchain de financiamento coletivo global para iniciar iniciativas de regeneração do mundo. Existe uma trend surgindo chamada REFI e é, a grosso modo, a tradução dos princípios ESG transpostos para projeto blockchain

A tecnologia blockchain pode permitir novas iniciativas ESG que antes não eram possíveis. Por exemplo, a blockchain pode ser usada para criar mercados descentralizados para produtos e serviços sustentáveis, permitindo que os consumidores comprem e vendam produtos que sejam ecologicamente corretos ou socialmente responsáveis. Isso pode ajudar a promover padrões sustentáveis de consumo e produção, levando a um futuro mais sustentável.

ESG é uma estrutura importante para promover investimentos sustentáveis e éticos, e as tecnologias que a blockchain traz podem garantir que os princípios ESG sejam devidamente empregados. Ao fornecer transparência, oportunidades alternativas de investimento, contratos inteligentes, a possibilidade do surgimento novas iniciativas descentralizadas e abordar os principais desafios dessa estratégia, além de oferecer modelos de organização descentralizados (DAOs) a tecnologia Blockchain se prova ser uma aliada extremamente poderosa das iniciativas ESG.

## **DAOs (Organizações Autônomas Descentralizadas)**

Disrupção significa uma ruptura tão abrupta que a maneira de fazer as coisas anteriormente deixam de fazer sentido. Da mesma maneira que o Bitcoin distribuiu o poder das criptomoedas não consagrou uma autoridade central e com isso deixou um legado ideológico.

A forma como as empresas operam comumente não faz sentido se comparada a maneira como a tecnologia Blockchain funciona. Por exemplo, a rede do Bitcoin fica mais forte à medida que outras pessoas se juntam justamente pela descentralização do poder.

Já existiam iniciativas de romper com as organizações tradicionais das

companhias, mas a blockchain trouxe a ideologia, os recursos de governança e pagamento necessários para a insurgência das Organizações autônomas descentralizadas.

### > O que são DAOs e como elas funcionam

DAO = Decentralized Autonomous Organization, ou seja, organização autônoma descentralizada.

Ao invés de chefes e supervisores, e uma hierarquia horizontal, as DAOs possuem um modelo de organização vertical. As DAOs são organizações que possuem pessoas trabalhando por um objetivo ou dentro de diretrizes em comum. Mediante as iniciativas propostas eles atuam podendo, qualquer um ser um iniciador de tarefas e contribuidor ativo.

Idealmente qualquer pessoa pode participar da iniciativa que desejar e ser recompensada de acordo com sua contribuição. Vale a pena mencionar que no cenário atual a maioria das organizações que se dizem DAOs ainda não atuam da maneira ideal.

Os motivos vão desde centralização do poder de votação deixando poucas pessoas (ou às vezes UMA) em cargo de realmente decidir o destino das atividades bem como, para alguns especialistas, o próprio ato de votar.

De acordo com Carl Amorim, um dos maiores especialistas em DAOs do mundo: 1, Se tem votação não é DAO! 2, Se tem fundo centralizado não é DAO!

Essa tese invalida todas as DAOs mas, mais que aplicar a risca vale a pena entender o que ele quer dizer com isso.

#### 1 - Se tem votação não é DAO!

A votação é um processo exclusivo onde 49% das pessoas podem ter que agir de maneira contrária a seu desejo e, mais que isso, se todos estão procurando atingir o mesmo objetivo, porque excluir QUALQUER um? De acordo com o especialista, o consenso precisa ser estabelecido pelos membros de maneira unânime.

## 2 - Se tem fundo centralizado não é DAO!

Os membros da DAO podem, eventualmente, investir seus fundos para operar ou prestar serviços, porém, qual seria o sentido de a votação da maioria decidir como meu dinheiro será empregado?

A proposta de Carl é simples. Dentro das DAOs devem existir múltiplas iniciativas e os envolvidos interagem com a rede para buscar recursos e dividir os frutos dessas iniciativas. Os membros que se interessarem pela iniciativa podem trabalhar na iniciativa e ou investir e dividir o valor recebido.

### > MakerDAO

MakerDAO é uma organização autônoma descentralizada (DAO) que opera na rede Ethereum. O objetivo da MakerDAO é criar uma stablecoin descentralizada chamada DAI, que é indexada ao dólar americano. DAI é criada através de um processo chamado "colateralização sobre garantia", que é administrado pelos usuários da plataforma.

O sistema da MakerDAO é composto por duas principais partes: a plataforma de empréstimos Collateralized Debt Position (CDP) e o token de governança Maker (MKR).

A plataforma de empréstimos CDP permite aos usuários depositar criptomoedas como garantia e criar DAI. O usuário deve depositar mais do que o valor atual do DAI para garantir que o valor da garantia seja maior do que o valor da dívida. Isso é conhecido como "colateralização sobre garantia". O usuário pode então usar o DAI para comprar outras criptomoedas ou usá-lo como uma stablecoin para outras transações. O token de governança Maker (MKR) é um token de utilidade que permite aos detentores votar sobre mudanças na plataforma. Os detentores de MKR são incentivados a manter a estabilidade da DAI, pois eles são penalizados financeiramente se a taxa de colateralização cair abaixo de um determinado limite. Isso é feito através de uma taxa de estabilidade chamada "taxa de estabilidade do sistema" (SF), que é definida pelos detentores de MKR. Uma das principais vantagens da MakerDAO é que ela é uma plataforma descentralizada, o que significa que não é controlada por uma única entidade. Isso ajuda a garantir a segurança e a transparência da plataforma,

já que todas as transações são registradas na rede Ethereum. Além disso, a MakerDAO fornece uma solução para a volatilidade do mercado de criptomoedas, permitindo que os usuários criem DAI que é indexada ao dólar americano.

No entanto, existem alguns desafios associados ao uso da MakerDAO. A principal preocupação é a possibilidade de queda dos preços das criptomoedas utilizadas como garantia. Se o preço dessas criptomoedas cair significativamente, os usuários podem não ser capazes de manter a colateralização sobre garantia necessária para manter a estabilidade da DAI.

Além disso, a governança não é devidamente distribuída e o voto do fundador geralmente resolve empates, conferindo a ele um poder de votação maior que qualquer outra parte da organização.