**Capítulo 21  
Finanças Descentralizadas**

Finanças descentralizadas é um novo sistema financeiro construído usando contratos inteligentes e a tecnologia blockchain que opera de maneira descentralizada sem depender de intermediários financeiros tradicionais.

Neste capítulo, cobriremos os seguintes tópicos:

* Introdução
* Mercados financeiros e negociação
* Aplicação da blockchain nas finanças
* Finanças descentralizadas
* Primitivos de DeFi
* Serviços de DeFi
* Benefícios de DeFi
* Usando o Uniswap

Agora, vamos ter uma breve introdução às finanças e aos mercados financeiros. Isso fornecerá uma base para o material apresentado a seguir, como o DeFi, já que muitos dos termos e ideias são os mesmos, embora em um contexto diferente.

**Introdução**  
Finanças é o estudo e a gestão de dinheiro, investimentos, a criação de dinheiro e outros instrumentos financeiros para maximizar a riqueza e minimizar o risco. O atual sistema financeiro global opera através de uma rede complexa de mercados financeiros, instituições e intermediários, com o objetivo de facilitar a alocação eficiente de recursos financeiros. Mercados financeiros, como bolsas de valores e mercados de títulos, servem como locais para compra e venda de ativos financeiros. Instituições financeiras, como bancos e empresas de investimento, desempenham um papel crucial intermediando entre tomadores e emprestadores e oferecendo serviços financeiros a seus clientes. Órgãos reguladores, como agências governamentais, são responsáveis por supervisionar e regular instituições e mercados financeiros para garantir sua operação segura e sólida e para proteger os consumidores. Investidores, como indivíduos, instituições e organizações, investem em ativos financeiros para gerar retornos e gerenciar riscos financeiros.

**<página seguinte>**

Todas essas entidades e componentes do atual sistema financeiro global trabalham juntos para promover estabilidade financeira, crescimento e prosperidade, e para atender às necessidades financeiras de indivíduos, empresas e da sociedade.

A indústria de serviços financeiros oferece uma gama diversificada de ativos e instrumentos financeiros para atender às necessidades de seus clientes. Por exemplo, ações, títulos, fundos mútuos e Fundos Negociados em Bolsa (ETFs); instrumentos do mercado monetário, como certificados de depósito; e derivativos, como opções e contratos futuros. Estes são apenas alguns dos muitos ativos e instrumentos financeiros oferecidos pela indústria de serviços financeiros.

Um mercado financeiro é uma plataforma onde instrumentos financeiros são negociados entre compradores e vendedores. Em um mercado financeiro, os preços dos ativos financeiros são determinados pela oferta e demanda e refletem as expectativas dos participantes do mercado quanto a eventos e condições futuras.

O sistema financeiro atual é centralizado e, tradicionalmente, todas as instituições financeiras mantêm a custódia dos fundos e ativos dos clientes. Elas também atuam como intermediárias para transações. Essa centralização significa que contas de clientes podem ser congeladas, a censura de transações pode ocorrer e as instituições podem cobrar de forma injusta pelos serviços prestados. Todas essas instituições financeiras são altamente regulamentadas e devem aderir a regras rigorosas de conformidade, como Conheça Seu Cliente (KYC), Prevenção à Lavagem de Dinheiro (AML) e Combate ao Financiamento do Terrorismo (CFT). Tais regulamentações oferecem confiança aos investidores e mantêm o sistema financeiro funcionando de forma eficiente; no entanto, observe que, por serem sistemas inerentemente centralizados, justiça, transparência, taxas competitivas e confiabilidade 100% não podem ser garantidas. Além disso, o cliente deve compartilhar detalhes pessoais e financeiros com esses prestadores de serviço e, como resultado, as instituições conhecem a identidade real e todo o histórico de contas e transações do cliente. Isso é aceitável e funciona razoavelmente bem no sistema financeiro atual; contudo, essa falta de privacidade pode não ser aceitável para alguns clientes. Além disso, o cliente está totalmente alheio ao que acontece a portas fechadas; há transparência limitada quando se trata de processamento de transações. Os clientes não sabem como seus dados são tratados ou como as transações são realizadas; tudo isso é opaco e significa que o sistema não é tão transparente quanto deveria ser. Os bancos de dados são opacos e isolados, e o compartilhamento de dados entre instituições se torna um problema. Os clientes, na maioria das vezes, estão totalmente desinformados sobre como seus dados e transações são tratados e processados. Isso significa que os clientes devem confiar totalmente nessas entidades centralizadas.

Observe que não é o caso de que o sistema financeiro atual esteja totalmente quebrado e nada funcione. O sistema financeiro atual funciona muito bem e, de fato, sustenta os mais altos padrões de qualidade, adesão à regulamentação e requisitos de conformidade, mas pode ser melhorado em termos de privacidade, inclusão financeira, transparência, confiança e eficiência.

Em 2008, uma invenção revolucionária, conhecida como Bitcoin, forneceu uma plataforma que poderia oferecer soluções para esses problemas. O Bitcoin (o primeiro sistema de dinheiro eletrônico totalmente ponto a ponto, que não precisa de uma terceira parte confiável para operar) introduziu a blockchain, que é a camada fundamental que pode fornecer soluções para a maioria, senão todos, desses problemas.

Agora vamos nos aprofundar e entender alguns dos conceitos das finanças tradicionais. Primeiro, vamos dar uma olhada nos mercados financeiros.

**Mercados financeiros**  
Mercados financeiros permitem a negociação de valores mobiliários, como títulos, ações, derivativos e moedas. Existem, de forma geral, três tipos de mercados: mercados monetários, mercados de crédito e mercados de capitais:

* **Mercados monetários** são mercados de curto prazo onde o dinheiro é emprestado para empresas ou bancos para empréstimos interbancários. O câmbio estrangeiro, ou forex, é outra categoria de mercados monetários onde moedas são negociadas.
* **Mercados de crédito** consistem principalmente de bancos de varejo que tomam dinheiro emprestado dos bancos centrais e o emprestam para empresas ou famílias na forma de hipotecas ou empréstimos.
* **Mercados de capitais** facilitam a compra e venda de instrumentos financeiros, principalmente ações e títulos. Existem muitos tipos de instrumentos financeiros, como instrumentos de caixa, instrumentos derivativos, empréstimos, valores mobiliários e muitos outros. A securitização é o processo de criação de um novo título transformando ativos ilíquidos em instrumentos financeiros negociáveis. Mercados de capitais podem ser divididos em dois tipos: mercados primários e mercados secundários. As ações são emitidas diretamente pelas empresas aos investidores nos mercados primários, enquanto nos mercados secundários, os investidores revendem seus títulos a outros investidores via bolsas de valores. Vários sistemas de negociação eletrônica são usados pelas bolsas atualmente para facilitar a negociação de instrumentos financeiros.

Uma atividade importante realizada nos mercados financeiros é a negociação, que discutiremos a seguir.

**Negociação**  
Um mercado é um local onde as partes se engajam em trocas. Pode ser tanto um local físico quanto eletrônico ou virtual. Vários instrumentos financeiros, incluindo ações, câmbio estrangeiro, commodities e vários tipos de derivativos são negociados nesses mercados.

Derivativos são contratos financeiros cujo valor deriva de um ativo subjacente, como ações, títulos, commodities, moedas ou índices. Eles são usados para proteger contra riscos, especular e gerenciar a exposição a movimentos de preços do ativo subjacente. Várias classes de derivativos incluem futuros, opções, swaps e contratos a termo. Eles são negociados nos mercados financeiros em bolsas organizadas, mercados de balcão (OTC) e várias plataformas eletrônicas de negociação. Quase todas as instituições financeiras introduziram plataformas eletrônicas de negociação para negociar vários tipos de instrumentos de diferentes classes de ativos.

**Bancos de varejo** são bancos comerciais que oferecem produtos e serviços financeiros a indivíduos e empresas, enquanto **bancos centrais** supervisionam o sistema monetário e a regulamentação do sistema financeiro de um país.

A negociação pode ser definida como uma atividade na qual operadores compram ou vendem vários instrumentos financeiros para gerar lucro e proteger-se contra riscos. Investidores, tomadores de empréstimos, hedgers, trocadores de ativos e especuladores são alguns tipos de operadores. Operadores têm uma **posição vendida** quando devem algo; em outras palavras, se venderam um contrato, estão com posição vendida. Quando compram um contrato, estão com **posição comprada**. Existem várias formas de realizar negociações, como por meio de corretores ou diretamente em uma bolsa ou OTC, onde compradores e vendedores negociam diretamente entre si em vez de usar uma bolsa. Corretores são agentes que organizam negociações para seus clientes e agem em nome do cliente para negociar a um preço dado ou ao melhor preço possível.

Operadores usam bolsas para executar funções de negociação como compra e venda de valores mobiliários, que introduziremos a seguir.

**Bolsas**  
Uma bolsa é uma plataforma centralizada onde valores mobiliários, commodities, derivativos e outros instrumentos financeiros são comprados e vendidos. Bolsas atuam como intermediárias entre compradores e vendedores de ativos financeiros, fornecendo um mercado padronizado e regulamentado para negociação. Elas garantem que as transações sejam executadas de maneira justa e transparente, fornecem dados de mercado e facilitam a liquidação das negociações. Alguns exemplos bem conhecidos de bolsas incluem a Bolsa de Valores de Nova York (NYSE), o Nasdaq, a Bolsa de Valores de Tóquio, a Bolsa de Valores de Londres e a Euronext. Cada bolsa é especializada na negociação de tipos específicos de valores mobiliários, como ações, títulos, futuros, opções ou moedas, e opera sob seu próprio conjunto de regras e regulamentos.

As bolsas geralmente são consideradas lugares muito seguros, regulamentados e confiáveis para negociar. Nas últimas décadas, a negociação eletrônica ganhou popularidade em relação à negociação tradicional realizada no piso da bolsa. Agora, os operadores enviam ordens a um livro central de ordens eletrônicas a partir do qual as ordens, preços e atributos relacionados são publicados para todos os sistemas associados usando redes de comunicação, criando, essencialmente, um mercado virtual. Negociações em bolsa só podem ser realizadas por membros da bolsa. Para negociar sem essas limitações, as contrapartes podem participar de negociações OTC diretamente.

Bolsas lidam com ordens; vamos agora explorar o que é uma ordem e suas várias propriedades.

**Ordens e propriedades das ordens**  
Ordens são instruções para negociar, e elas são os blocos de construção principais de um sistema de negociação. Elas têm os seguintes atributos gerais:

* O nome do instrumento
* A quantidade a ser negociada
* Direção (compra ou venda)
* O tipo de ordem que representa várias condições, por exemplo, ordens limitadas e ordens de parada

Em finanças, uma **ordem limitada** é um tipo de ordem que permite a venda ou compra de um ativo a um preço específico ou melhor. Uma **ordem de parada** é semelhante, mas a diferença fundamental é que uma ordem limitada é visível para o mercado, enquanto uma ordem de parada só se torna ativa (como uma ordem de mercado) quando o preço de parada especificado é atingido.

As ordens são negociadas por preços de compra (bid) e preços de venda (offer). Os operadores demonstram sua intenção de comprar ou vender anexando preços de bid e offer às suas ordens. O preço pelo qual um operador comprará é conhecido como preço de bid. O preço pelo qual um operador está disposto a vender é conhecido como preço de offer.

Para facilitar o manuseio correto das ordens, são utilizados sistemas de gerenciamento e roteamento de ordens, que introduziremos a seguir.

**Sistemas de gerenciamento e roteamento de ordens**  
Sistemas de roteamento de ordens encaminham e entregam ordens a vários destinos, dependendo da lógica de negócios. Os clientes os utilizam para enviar ordens a seus corretores, que então enviam essas ordens a negociantes, câmaras de compensação e bolsas.

Existem diferentes tipos de ordens. As duas mais comuns são as ordens de mercado e as ordens limitadas. Uma **ordem de mercado** é uma instrução para negociar ao melhor preço atualmente disponível no mercado. Essas ordens são executadas imediatamente a preços de mercado.

Em finanças, o **preço à vista (spot price)** é o preço atual de um ativo em um mercado onde ele pode ser comprado ou vendido para entrega imediata.

Por outro lado, uma **ordem limitada** é uma instrução para negociar ao melhor preço disponível, mas apenas se não for inferior ao preço limite definido pelo operador. Isso também pode ser maior, dependendo da direção da ordem: seja para vender ou comprar. Todas essas ordens são gerenciadas em um **livro de ordens**, que é uma lista de ordens mantida pela bolsa, e que registra a intenção de comprar ou vender por parte dos operadores.

Uma **posição** é um compromisso de vender ou comprar um número de instrumentos financeiros, incluindo valores mobiliários, moedas e commodities por um preço determinado. Os contratos, valores mobiliários, commodities e moedas que os operadores compram ou vendem são geralmente conhecidos como **instrumentos de negociação**, e eles estão sob o amplo guarda-chuva das **classes de ativos**. As classes mais comuns são ativos reais, ativos financeiros, contratos derivativos e contratos de seguros.

Uma negociação é composta por vários elementos, que discutiremos a seguir.

**Componentes de uma negociação**  
Um **bilhete de negociação** é a combinação de todos os detalhes relacionados a uma negociação. No entanto, há alguma variação dependendo do tipo do instrumento e da classe de ativos. Esses elementos são descritos a seguir.

Primeiramente, temos o **instrumento subjacente** que é a base da negociação. Pode ser uma moeda, um título, uma taxa de juros, uma commodity ou uma ação.

Os atributos dos instrumentos financeiros incluem:

* **Atributos gerais**: Isso inclui informações gerais de identificação e características essenciais associadas a toda negociação. Atributos típicos incluem um ID único, nome do instrumento, tipo, status, data de negociação e hora.
* **Economia**: A economia refere-se às características relacionadas ao valor da negociação; por exemplo, o valor de compra ou venda, código do ativo (ticker), bolsa, preço e quantidade.
* **Vendas**: Refere-se aos detalhes relacionados às características de vendas, como o nome do vendedor. É apenas um campo informativo, geralmente sem impacto no ciclo de vida da negociação.
* **Contraparte**: A contraparte é um componente essencial de uma negociação, pois mostra o outro lado (a outra parte envolvida na negociação), e é necessário para liquidar a negociação com sucesso. Os atributos normais incluem nome da contraparte, endereço, tipo de pagamento, IDs de referência, data de liquidação e tipo de entrega.

**Ciclo de vida da negociação**  
Um ciclo de vida geral de uma negociação inclui várias etapas, desde o envio da ordem até a execução e a liquidação. Esse ciclo de vida é descrito passo a passo a seguir:

* **Pré-execução**: Uma ordem é enviada nesta etapa.
* **Execução e registro**: Quando a ordem é casada e executada, ela se converte em uma negociação. Neste estágio, o contrato entre as contrapartes é firmado.
* **Confirmação**: É quando ambas as contrapartes concordam com os detalhes da negociação.
* **Pós-registro**: Esta etapa diz respeito a vários processos de verificação e escrutínio exigidos para verificar a exatidão da negociação.
* **Liquidação**: Esta é a parte mais vital do ciclo de vida da negociação. Nesta etapa, a negociação é concluída.
* **Processamento de final de dia**: Os processos de final de dia incluem geração de relatórios, cálculo de lucros e perdas, e vários cálculos de risco.

Esse ciclo de vida também é mostrado na imagem a seguir:

**<IMAGEM>**

Em todos os processos mencionados anteriormente, muitas pessoas e funções de negócios estão envolvidas. Comumente, estas são divididas em funções como **front office**, **middle office** e **back office**.

Embora a indústria de negociação seja muito segura e funcione bem, há alguns problemas que podem ocorrer. Um deles é a **antecipação de ordens**, onde antecipadores tentam obter lucro antes que outros operadores possam realizar negociações. Isso se baseia na antecipação por parte de um operador que sabe como as atividades de outros operadores afetarão os preços. Front-runners, operadores técnicos orientados por sentimento e manipuladores são alguns exemplos de antecipadores de ordens.

Além disso, há a possibilidade de **manipulação de mercado**. Isso é estritamente ilegal em todos os países. Operadores fraudulentos podem espalhar informações falsas no mercado, o que pode resultar em movimentos de preços, possibilitando lucros ilícitos. Geralmente, a conduta de manipulação de mercado é baseada em negociações, e inclui manipulações generalizadas e específicas no tempo. Ações que podem criar uma escassez artificial de ações, uma impressão de atividade falsa e manipulação de preços para obter ganhos criminosos estão incluídas nessa categoria.

Ambos os conceitos são relevantes para crimes financeiros. No entanto, é possível desenvolver sistemas baseados em blockchain que possam impedir abusos de mercado devido às suas propriedades inerentes de **transparência e segurança**.

**Aplicações da blockchain nas finanças**  
Percebeu-se rapidamente, após a invenção do Bitcoin, que a blockchain pode permitir muitos casos de uso na indústria de serviços financeiros que podem trazer eficiência, transparência e segurança. Apresentamos alguns desses casos de uso a seguir e exploramos qual impacto a blockchain tem nas finanças tradicionais e como ela melhora os serviços existentes. Após esta seção, entraremos em finanças descentralizadas, também conhecidas como **DeFi**.

A blockchain possui muitas aplicações potenciais na indústria financeira. Atualmente, blockchain nas finanças é o tema mais quente do setor, e grandes bancos e organizações financeiras estão pesquisando maneiras de adotar a tecnologia blockchain, principalmente por seu potencial altamente desejável de reduzir custos. Essas aplicações incluem, mas não se limitam a: pagamentos, pagamentos transfronteiriços, remessas, financiamento comercial, financiamento da cadeia de suprimentos, negociação de valores mobiliários, compensação e liquidação, contabilidade, identidade, KYC e AML, seguros, liquidações pós-negociação, prevenção de crimes financeiros, empréstimos e financiamentos. Discutimos alguns desses a seguir.

**Seguros**  
Na indústria de seguros, a tecnologia blockchain pode ajudar a impedir reivindicações fraudulentas, aumentar a velocidade do processamento de sinistros e permitir transparência. Imagine um livro-razão compartilhado entre todas as seguradoras que possa fornecer um mecanismo rápido e eficiente para lidar com sinistros entre empresas. Além disso, com a convergência da IoT e da blockchain, pode-se imaginar um ecossistema de dispositivos inteligentes, onde todas essas coisas podem negociar e gerenciar suas apólices de seguro, que são controladas por contratos inteligentes na blockchain.

A blockchain pode reduzir o custo geral e o esforço necessários para processar sinistros. Reivindicações podem ser automaticamente verificadas e pagas via contratos inteligentes e a identidade associada do segurado. Por exemplo, um contrato inteligente, com a ajuda de um oráculo e possivelmente IoT, pode garantir que, quando um acidente ocorrer, ele registre os dados de telemetria relacionados e, com base nessas informações, libere o pagamento. Também pode reter o pagamento se o contrato inteligente, após avaliar as condições de pagamento, concluir que o pagamento não deve ser liberado; por exemplo, em um cenário onde uma oficina autorizada não consertou o veículo ou foi usada fora de uma área designada, e assim por diante. Podem haver muitas condições que um contrato inteligente pode avaliar para processar sinistros, e a escolha dessas regras depende da seguradora, mas a ideia geral é que contratos inteligentes, em combinação com IoT e oráculos, podem automatizar toda a indústria de seguros de veículos.

**Liquidação pós-negociação**  
Esta é a aplicação mais cobiçada da tecnologia blockchain. Atualmente, muitas instituições financeiras estão explorando a possibilidade de usar tecnologia blockchain para simplificar, automatizar e acelerar o processo de liquidação pós-negociação, que é caro e demorado.

Para entender melhor o problema, o ciclo de vida de uma negociação será descrito brevemente. Um ciclo de vida de negociação contém três etapas: execução, compensação e liquidação. A execução está relacionada ao compromisso de negociação entre duas partes e pode ser inserida no sistema via terminais de gerenciamento de ordens do front office ou bolsas. A compensação é o próximo passo, no qual a negociação é casada entre o vendedor e o comprador com base em certos atributos, como preço e quantidade.

Nesta etapa, as contas envolvidas no pagamento também são identificadas. Finalmente, a liquidação é onde, eventualmente, o valor mobiliário é trocado por pagamento entre o comprador e o vendedor.

No modelo tradicional de ciclo de vida da negociação, uma **câmara de compensação central** é necessária para facilitar a negociação entre as partes, que assume o risco de crédito de ambas as partes. O esquema atual é um tanto complicado, no qual um vendedor e um comprador devem seguir uma rota complicada para negociar entre si. Isso envolve várias empresas, corretores, câmaras de compensação e custodiantes, mas com a blockchain, um único livro-razão distribuído com contratos inteligentes apropriados pode simplificar todo esse processo e permitir que compradores e vendedores se comuniquem diretamente entre si.

Notavelmente, o processo de liquidação pós-negociação geralmente leva de dois a três dias e depende de câmaras de compensação centrais e sistemas de reconciliação. Com a abordagem de livro-razão compartilhado, todos os participantes na blockchain podem ver imediatamente uma versão única e verdadeira do estado da negociação. Além disso, a liquidação P2P é possível, o que resulta na redução da complexidade, custo, risco e do tempo necessário para liquidar a negociação. Finalmente, intermediários podem ser eliminados utilizando contratos inteligentes apropriados na blockchain. Reguladores também podem visualizar a blockchain para requisitos de auditoria e regulamentação.

**Prevenção de crimes financeiros**  
KYC e AML são os principais habilitadores para a prevenção de crimes financeiros. No caso do KYC, atualmente, cada instituição mantém sua própria cópia dos dados do cliente e realiza a verificação via fornecedores de dados centralizados. Isso pode ser um processo demorado e resultar em atrasos na integração de um novo cliente.

A blockchain pode fornecer uma solução para esse problema ao compartilhar com segurança um livro-razão distribuído entre todas as instituições financeiras que contenha identidades verificadas e verdadeiras dos clientes. Esse livro-razão distribuído só pode ser atualizado por consenso entre os participantes, proporcionando, assim, transparência e auditabilidade. Isso pode não apenas reduzir custos, mas também permitir que requisitos regulatórios e de conformidade sejam atendidos de maneira melhor e mais consistente.

No caso do AML, devido à natureza imutável, compartilhada e transparente da blockchain, os reguladores podem ser facilmente autorizados a acessar uma blockchain privada, onde podem obter dados para relatórios regulatórios relevantes. Isso também resultará na redução da complexidade e dos custos relacionados ao paradigma atual de relatórios regulatórios. No modelo atual, os dados são extraídos de vários sistemas legados e díspares e depois agregados e formatados para fins de relatório. A blockchain pode fornecer uma visão compartilhada única de todas as transações financeiras no sistema, que são criptograficamente seguras, autênticas e auditáveis, reduzindo assim os custos e a complexidade associados aos métodos atualmente empregados. Uma solução simples é mostrada na Figura 21.2:

**<IMAGEM>**

A KYC baseada em blockchain é muito mais eficiente do que a KYC tradicional. Em um sistema tradicional, um cliente submete documentos/dados KYC a um banco. O banco verifica e armazena os dados e também os envia a um intermediário centralizado de terceiros para armazenamento. Outros bancos realizam o mesmo processo e/ou solicitam dados do intermediário centralizado, o que não é eficiente. Na maioria dos casos, os processos KYC atuais são isolados, e os bancos executam esse processo individualmente. Normalmente, todas as instituições mantêm seus próprios bancos de dados com pouca ou nenhuma troca de informações. Em alguns casos, há também um registro centralizado, mas, por ser centralizado, ele não possui os benefícios que acompanham a descentralização. Como resultado dessa situação complexa, a integração de clientes leva muito tempo — pode levar até dois meses em alguns casos. Também resulta em duplicação de esforços, pois cada banco precisa realizar sua própria KYC. Na KYC baseada em blockchain, um cliente submete seus dados KYC à blockchain. Uma instituição verifica os dados KYC e publica o status KYC na blockchain para aquele cliente. O cliente recebe o status compatível com o KYC (na forma de uma credencial verificável ou algum outro meio).

Bancos e outras instituições acessam os dados KYC da blockchain sem precisar solicitá-los a outras instituições, e o cliente pode apresentar a credencial verificável emitida a qualquer outra instituição como prova de que já passou pelo processo de KYC e não precisa fazê-lo novamente. Isso significa que outros bancos podem reutilizar os dados KYC, sem duplicação, e podem até usar credenciais verificáveis para verificar (sem nem mesmo ver os dados do cliente) que o cliente já está em conformidade com o KYC e pode acessar serviços financeiros. Tudo isso é possível graças à blockchain.

**Pagamentos**  
Um pagamento é a transferência de dinheiro ou seu equivalente de uma parte (o pagador) para outra (o beneficiário) em troca de serviços, bens ou para cumprir um contrato. Os pagamentos geralmente são feitos na forma de dinheiro, transferências bancárias, pagamentos com cartão de crédito e cheques. Existem vários sistemas eletrônicos de pagamento em uso, como o **Bankers’ Automated Clearing System (BACS)** e o **Clearing House Automated Payment System (CHAPS)**. Todos esses sistemas, no entanto, são centralizados e regidos por códigos e práticas tradicionais da indústria de serviços financeiros. Esses sistemas funcionam adequadamente, mas com o advento da blockchain, surgiu o potencial tecnológico de resolver algumas das limitações que existem nos sistemas atualmente utilizados.

As principais vantagens que a tecnologia blockchain pode trazer para os pagamentos são: **descentralização**, **tempos de liquidação mais rápidos**, **maior resiliência** e **alta disponibilidade**. Com todas essas vantagens, é fácil ver como a indústria de pagamentos pode se beneficiar da tecnologia blockchain. Existe também outro ramo dos pagamentos que lida com **pagamentos internacionais ou transfronteiriços**, que apresenta seus próprios desafios. Na finança tradicional, o pagamento transfronteiriço é um processo complexo que pode levar dias para ser processado e envolve múltiplos intermediários. Os mecanismos atuais sofrem com atrasos causados por vários intermediários, aplicação de regulamentações, diferenças entre regulamentações de diferentes jurisdições... a lista continua. Todos esses problemas podem ser resolvidos utilizando tecnologia blockchain. A vantagem mais significativa é a **descentralização**, onde, devido à ausência da necessidade de intermediários, os pagamentos podem ser feitos diretamente entre empresas ou indivíduos. Além disso, devido à conectividade P2P, todo o processo torna-se muito mais rápido — quase instantâneo, de fato — o que resulta em maior produtividade e agilidade nos negócios. Podemos ver, na Figura 21.3, como um sistema complexo pode ser transformado em um sistema mais simples usando blockchain.

**<IMAGEM>**

O uso da blockchain no sistema de pagamentos transfronteiriços elimina riscos de liquidação. O beneficiário recebe os fundos em segundos/minutos em vez de dias, mesmo para pagamentos internacionais. Além disso, é de baixo custo, pois não há bancos intermediários que possam cobrar taxas. Também não há necessidade de reconciliação, já que todos os dados estão na cadeia, já verificados, e todos os participantes podem vê-los e usá-los. Não há horários de corte ou atrasos devido a feriados etc., pois o sistema funciona 24 horas por dia, 7 dias por semana, desde que a blockchain esteja em execução. Ele também possibilita pagamentos **Peer-to-Peer (P2P)**, nos quais pagadores e beneficiários podem lidar diretamente entre si por meio de carteiras conectadas à blockchain, sem intermediários. Em alguns casos, devido a requisitos regulatórios, instituições podem ser necessárias, mas, ainda assim, a experiência geral para um cliente é muito mais fácil, rápida e fluida.

Mais e mais casos de uso estão surgindo: **compensação e liquidação**, **identidade**, **mercados primário e secundário**, **financiamento comercial**, **cadeia de suprimentos**, e muitos outros. Está agora claro que a blockchain realmente possibilita casos de uso que antes não eram possíveis.

Embora a maioria das inovações discutidas até agora seja baseada em blockchains com permissão (**permissioned**) e vise melhorar os processos financeiros existentes ao implementá-los em blockchains, surgiu outro fenômeno chamado **finanças descentralizadas em blockchains públicas**.

Vamos agora explorar o que é o DeFi.

**Finanças Descentralizadas**  
Podemos definir **DeFi** como um mecanismo financeiro construído usando contratos inteligentes em blockchains públicas com o objetivo de fornecer serviços financeiros tradicionais e inovadores de forma descentralizada, sem confiança, interoperável e sem permissão.

Enquanto as Finanças Tradicionais (**TradFi**) — ou Finanças Centralizadas (**CeFi**) — buscaram durante décadas alcançar eficiência e melhorar seus serviços (e conseguiram bastante), o **DeFi**, no entanto, devido às vantagens da blockchain, pode resultar em uma transformação total dos serviços financeiros no futuro, e possibilitou (e está possibilitando e continuará a possibilitar) casos de uso que nunca foram possíveis antes da invenção da blockchain. Trata-se de um ecossistema que surgiu como resultado do desenvolvimento de diversos tipos de aplicações financeiras construídas sobre blockchains. Com as blockchains sendo descentralizadas e as aplicações relacionadas a finanças, surgiu o termo **finanças descentralizadas**, ou **DeFi**.

DeFi pode ser definido como um termo guarda-chuva usado para descrever um ecossistema de serviços financeiros construído sobre blockchains. Finanças Centralizadas (**CeFi**) é o termo agora usado para se referir à indústria de serviços financeiros tradicional, que é centralizada por natureza, enquanto **DeFi** é um movimento para descentralizar a indústria tradicional de serviços financeiros centralizados.

A **tokenização** desempenha um papel vital no ecossistema DeFi. O DeFi é baseado na tokenização de ativos. Discutimos a tokenização em detalhes no **Capítulo 15, Tokenização**. O DeFi é um assunto vasto com muitas aplicações, protocolos, ativos, tokens, blockchains e contratos inteligentes.

O ecossistema DeFi é a infraestrutura que mais cresce atualmente, executando-se em diferentes blockchains. Originalmente, a maioria das aplicações DeFi rodava no **Ethereum**, mas com o advento de novas cadeias como **Solana, Cosmos, Polkadot, Avalanche, EOS, Hedera**, e muitas outras, vemos uma expansão exponencial do ecossistema DeFi. No entanto, o Ethereum continua sendo o mais preferido. O DeFi está possibilitando casos de uso que são inovadores e que simplesmente não eram possíveis antes.

A gama de DApps DeFi inclui, mas não se limita a: empréstimos e financiamentos, negociação, gerenciamento de ativos, seguros, tokenização e mercados de previsão. Todas essas aplicações descentralizadas, juntamente com seus contratos inteligentes e infraestrutura, compõem o ecossistema DeFi.

Para determinar se uma aplicação ou protocolo é realmente um protocolo DeFi, podemos fazer três perguntas:

1. O usuário tem controle total do ativo financeiro?
2. Uma única entidade pode censurar transações?
3. Uma única entidade pode censurar a execução do protocolo?

Se a resposta a todas essas perguntas for **não**, então o DApp é de fato um verdadeiro DApp DeFi. Se a resposta a qualquer uma das perguntas for **sim**, então não se trata de uma verdadeira aplicação ou protocolo DeFi.

Vamos agora comparar finanças centralizadas com finanças descentralizadas, o que ajuda a entender como o DeFi difere do CeFi.

| **CeFi** | **DeFi** |
| --- | --- |
| **Admissão** | Com permissão |
| **Camada base** | Bancos de dados centralizados |
| **Autorização** | Requerida |
| **Custódia de ativos** | Custodial – terceira parte confiável |
| **Confiança** | Centralizada |
| **Governança** | Centralizada – sob o controle de uma única parte |
| **Privacidade** | Limitada, identidade real deve ser revelada via KYC/AML |
| **Transparência** | Opaca |
| **Risco** | Menos arriscado (plataformas estáveis, regulamentação) |
| **Acessibilidade** | Restrita por regulamentações, políticas etc. |

**Propriedades do DeFi**

O DeFi deve demonstrar cinco propriedades-chave, incluindo:

* **Não custodial**: os usuários têm controle total sobre seus ativos.
* **Sem permissão**: o sistema é totalmente inclusivo e qualquer pessoa pode acessar serviços financeiros.
* **Descentralizado**: não há autoridade única no controle da plataforma, do protocolo ou da execução de transações. Em outras palavras, não há exigência de terceiros confiáveis.
* **Transparente**: o sistema é aberto à auditoria e inspeção por qualquer pessoa para garantir sua integridade.
* **Componível**: o sistema permite a criação de novos produtos financeiros a partir de alguns blocos básicos.

**O ChatGPT disse:**

**Camadas do DeFi**

O ecossistema DeFi pode ser descrito em termos de uma arquitetura em camadas, onde cada camada representa uma classe de operações e tecnologias.

Vamos ver cada uma dessas camadas uma por uma:

1. **Camada de liquidação (Settlement layer)**: Esta é a camada base onde plataformas blockchain como Ethereum, Solana e Polkadot existem.
2. **Camada de ativos (Asset layer)**: Esta camada é composta por tokens e criptomoedas, tokens nativos, stablecoins, NFTs e outros tokens – por exemplo, ERC20 e ERC721.
3. **Camada de protocolo (Protocol layer)**: Esta camada consiste em protocolos DeFi incluindo exchanges, plataformas de empréstimo, plataformas de seguros DeFi e muitos outros protocolos. Esta camada é implementada usando contratos inteligentes. Mais especificamente, Organizações Autônomas Descentralizadas (**DAOs**) existem nesta camada.
4. **Camada de aplicação (Application layer)**: Esta camada é composta por aplicações descentralizadas que rodam sobre os protocolos da camada de protocolo e incluem aplicações e interfaces.
5. **Camada de interoperabilidade (Interoperability layer)**: Esta camada é responsável por fornecer interoperabilidade entre cadeias (cross-chain), o que inclui pontes (bridges), hubs, cadeias de retransmissão (relay chains) e vários protocolos de mensagens cross-chain.
6. **Camada de agregação (Aggregation layer)**: Esta camada introduz a capacidade de agregar múltiplas aplicações em uma única plataforma fácil de usar para usuários finais.

Podemos visualizar essa arquitetura em camadas com diferentes atores e entidades na **Figura 21.4** abaixo:

**<IMAGEM>**

Cada camada no ecossistema DeFi desempenha um papel crucial na viabilização da criação e crescimento de aplicações e serviços financeiros descentralizados. O ecossistema DeFi tem o potencial de oferecer maior acesso e inclusão financeira, assim como novas oportunidades e inovações financeiras. No entanto, é importante observar que o DeFi está evoluindo rapidamente, e existem alguns riscos e incertezas associados à participação no ecossistema DeFi. Cobriremos esses riscos mais adiante neste livro, quando discutirmos segurança em blockchain e outros desafios.

**Primitivos do DeFi**

O ecossistema DeFi é composto por muitos protocolos, serviços, atores e entidades. Esses elementos estão listados abaixo:

* **Transações e contratos inteligentes**: Transações e contratos inteligentes são o bloco de construção básico sobre o qual o DeFi opera. A funcionalidade de transações e contratos inteligentes é fornecida pela blockchain subjacente, como o Ethereum.
* **Keepers**: *Keepers* podem ser definidos como uma classe de contas controladas externamente (**EOAs – External Owned Accounts**) que possuem incentivo para realizar uma ação em um protocolo DeFi. Um *keeper* também pode ser um agente autônomo ou um bot que monitora e aciona certas ações com base em condições específicas dentro de um contrato inteligente, e ganha recompensas por isso. *Keepers* atuam como a "equipe de manutenção" do ecossistema DeFi, monitorando continuamente o estado dos contratos inteligentes e executando transações ou atividades predefinidas quando certas condições são atendidas. Por exemplo, um *keeper* pode monitorar um protocolo de empréstimo e automaticamente quitar um empréstimo em nome do mutuário se ele cair abaixo de um certo índice de colateralização. *Keepers* ajudam a manter a saúde e a estabilidade dos protocolos DeFi e são geralmente incentivados com recompensas por seus serviços.
* **Token**: Um token é uma representação digital de um ativo, como uma criptomoeda, uma mercadoria, uma ação ou uma moeda fiduciária. Esses tokens são criados e gerenciados em uma blockchain e são usados como meio de troca, reserva de valor, mecanismo de governança ou para outras funções dentro de protocolos DeFi. Tokens podem ser usados em uma variedade de protocolos DeFi, como exchanges descentralizadas e plataformas de empréstimo. Eles também podem ser usados para incentivar usuários a participarem desses protocolos ou como direito de voto em decisões de governança dentro do protocolo. Alguns dos tokens populares usados em protocolos DeFi incluem **stablecoins** como USDC, DAI e USDT, e tokens de governança como UNI, AAVE e DOT. Para mais detalhes sobre tokenização, consulte o **Capítulo 15, Tokenização**, que abordou esse assunto em detalhes.
* **Oráculo (Oracle)**: Um oráculo pode ser definido como um mecanismo que fornece informações externas do mundo real para a blockchain. Ele desempenha um papel vital no ecossistema DeFi. Por exemplo, permite a criação de aplicações que requerem dados em tempo real, como exchanges descentralizadas, plataformas de empréstimos e protocolos de seguros.
* **Governança**: Governança refere-se ao processo de tomada de decisões para gerenciar e evoluir um protocolo descentralizado. É tipicamente alcançada por meio de consenso entre os participantes, como detentores de tokens, que expressam suas preferências por meio de mecanismos de votação. DAOs são um mecanismo comum usado em protocolos DeFi para governança. A governança pode incluir decisões sobre mudanças técnicas, incentivos econômicos e adição ou remoção de funcionalidades no protocolo. A governança descentralizada permite a criação de protocolos DeFi mais abertos, transparentes e democráticos, controlados pelos usuários em vez de intermediários centralizados ou terceiros confiáveis.

Dando continuidade à seção **Primitivos do DeFi**:

* **Custódia (Custody)**: A custódia é um primitivo fundamental no DeFi que permite aos usuários escorar ou manter fundos em um contrato inteligente. Tal custódia possibilita a criação de diferentes soluções, especialmente **protocolos de empréstimo**, **fundos de seguros**, **formação de mercado** e **distribuição automatizada de incentivos**.
* **Incentivo (Incentive)**: Incentivos no ecossistema DeFi desempenham um papel importante na manutenção da lucratividade para os usuários. Um tipo comum é o incentivo por staking, no qual um usuário **bloqueia alguns ativos** para **proteger ou participar da governança** de um protocolo DeFi e **ganhar recompensas** como retorno. Vale notar que os incentivos podem ser reduzidos ou aumentados em um protocolo com base no comportamento do usuário, nas condições de mercado e nas regras do protocolo. Os incentivos podem ser **negativos ou positivos** – por exemplo, uma recompensa de staking é um **incentivo positivo** obtido ao contribuir com ativos em um protocolo para protegê-lo. **Incentivos negativos** podem ocorrer devido a regras de penalização codificadas em um protocolo, usadas para **desencorajar comportamentos indesejáveis** dos participantes.
* **Ponte (Bridge)**: Uma ponte é um mecanismo que conecta duas redes blockchain separadas, permitindo que **ativos e dados sejam transferidos entre elas**. Pontes são importantes para possibilitar a interoperabilidade entre diferentes ecossistemas DeFi, pois permitem que os usuários movimentem ativos e dados entre diferentes redes. As pontes podem ser implementadas como trocas atômicas entre cadeias (**cross-chain atomic swaps**), encapsulamento de tokens (**token wrapping**), ou por meio de **protocolos de ponte** que usam um conjunto de contratos inteligentes para facilitar a transferência ou troca de ativos entre redes blockchain. Algumas pontes comuns são a ponte **Ethereum–Binance Smart Chain**, a ponte **Ethereum–Polygon** e a ponte **Ethereum–Polkadot**. Pontes são importantes para expandir a funcionalidade e o alcance do DeFi, pois permitem que ativos e liquidez sejam movidos entre diferentes redes blockchain, facilitando o acesso dos usuários a uma gama mais ampla de aplicações e serviços DeFi.

**Serviços DeFi**

O DeFi é composto por muitos protocolos diferentes, componentes e serviços. Discutimos esses serviços a seguir.

**Tokenização de ativos**

Essa é a **fundação sobre a qual o DeFi é construído**. Trata-se do processo de adicionar novos ativos a uma plataforma blockchain. Podemos pensar em um token como uma **representação digital de um ativo do mundo real**. A tokenização torna os ativos mais acessíveis, programáveis, flexíveis e fáceis de transferir. Existem muitos tipos de tokens, incluindo **tokens de segurança**, **tokens de governança**, **NFTs**, **stablecoins**, e vários outros. Para mais detalhes sobre tokenização, consulte o **Capítulo 15, Tokenização**, onde esses conceitos são explicados em detalhes.

**A tokenização pode tornar ativos ilíquidos em líquidos**, o que não é possível pelos meios tradicionais.  
*Exemplo: tokenizar uma obra de arte famosa.*

**Exchanges descentralizadas**

Podemos dividir as exchanges em dois tipos: **exchanges centralizadas** e **exchanges descentralizadas**.

Uma exchange é, tradicionalmente, **centralizada**, o que significa que algumas delas podem não ser totalmente confiáveis. Elas não são transparentes, e a custódia também é centralizada. Vimos como exchanges centralizadas de criptomoedas foram alvo de **ataques e práticas indevidas**, resultando na perda de **bilhões em fundos**. Por exemplo, **Mt. Gox**, **Coincheck** e **Binance** sofreram perdas devido a ataques bem-sucedidos no passado.

Uma **Exchange Descentralizada (DEX)** alivia os problemas enfrentados por uma **Exchange Centralizada (CEX)**. Podemos definir uma DEX como um tipo de exchange de criptomoedas (token) que opera em uma blockchain. DEXs permitem a **troca direta de criptomoedas entre usuários (pares)**, sem a necessidade de uma autoridade central ou intermediários. Isso contrasta com as exchanges centralizadas, que atuam como intermediárias e **custodiantes dos ativos** de seus usuários.

No DeFi e nos sistemas de negociação baseados em blockchain em geral, a negociação de tokens é a principal atividade. Tokens podem ser negociados em exchanges. Com o surgimento do DeFi, surgiram as **exchanges descentralizadas**. DEXs são descentralizadas e, portanto, não requerem nenhuma autoridade central ou intermediário para facilitar a negociação. São **transparentes**, **não custodiais** e **descentralizadas**.

Embora a barreira de entrada para DEXs seja baixa devido à ausência de exigências regulatórias tradicionais, como **KYC**, isso também as torna **arriscadas para investidores**, pois, se a DEX for hackeada, **não há proteção contra a perda de fundos**. KYC é uma prática padrão de diligência na indústria de serviços financeiros que garante que o cliente é legítimo e genuíno. No entanto, algumas exchanges cripto centralizadas já começaram a aplicar verificações de KYC e AML.

Alguns exemplos de DEXs são: **Uniswap**, **Bancor**, **WavesDEX**, **0x** e **IDEX**. Esse ecossistema está crescendo a um ritmo muito acelerado e espera-se que continue a crescer ainda mais.

**A estrutura básica de uma DEX**

A estrutura básica de uma DEX é composta por um **contrato inteligente** que facilita a negociação entre duas partes. Esse contrato inteligente consiste em três funções:

* **Descoberta de preços (price discovery)**
* **Casamento de ordens (trade matching)**
* **Liquidação da negociação (trade clearing)**

Podemos visualizar isso na **Figura 21.5** abaixo:

**<IMAGEM>**

A descoberta de preços é o processo de determinar o valor justo de mercado de um ativo financeiro por meio das forças de **oferta e demanda no mercado**. Ela ajuda a estabelecer o preço pelo qual um comprador e um vendedor estão dispostos a negociar o ativo e garante que os ativos sejam precificados de forma justa e precisa. A descoberta de preços ocorre por meio de vários mecanismos, como negociações em exchanges, transações OTC e uso de derivativos, sendo influenciada por dados econômicos, eventos geopolíticos e sentimento de mercado. É essencial para a alocação eficiente de capital e risco nos mercados financeiros.

**Tipos de DEXs**

Existem vários tipos de DEXs, incluindo:

1. **Formador de Mercado Automatizado (AMM)** – também chamado de DEX baseado em pool de liquidez
2. **DEX baseado em livro de ordens**  
   a. Livro de ordens on-chain  
   b. Livro de ordens off-chain
3. **Agregadores de DEX (DEX aggregators)**

**Formador de Mercado Automatizado (AMM)**

Um AMM é um tipo de DEX onde um **pool de liquidez** fornece a base para a formação automatizada de mercado. Em um pool de liquidez, a formação de mercado é automatizada usando um **contrato inteligente**. Um usuário com tokens (ativos) adiciona liquidez ao pool, que pode consistir de vários ativos.

Qualquer operador que usar o pool de liquidez para **trocar ativos** paga uma taxa ao usuário que forneceu liquidez, adicionando seus tokens ao pool. A ideia central por trás do AMM é permitir que **contratos inteligentes realizem a formação de mercado** em vez de os usuários colocarem ordens manualmente. Em resumo, **pools de liquidez** podem ser pensados como “potes” compartilhados de fundos usados pelas DEXs, depositados pelos usuários da DEX, chamados de **provedores de liquidez**. Pools de liquidez são usados pelas DEXs para **comprar, vender e cumprir ordens**. Provedores de liquidez ganham taxas do pool em troca de travar fundos no pool, em um processo chamado de **mineração de liquidez (liquidity mining)**.

**Modelos de AMM**

Os AMMs utilizam **fórmulas matemáticas** para ajustar os preços no pool de liquidez. Essa fórmula é programada no contrato inteligente. Existem vários **modelos de formador de mercado de função constante (CFMM – Constant Function Market Maker)**, incluindo **CPMM**, **CSMM** e **CMMM**.

**CPMM (Constant Product Market Maker)**

A fórmula de produto constante é simplesmente o produto de dois ativos, conforme mostrado na equação abaixo:

  x \* y = k

Onde x representa a quantidade de um ativo x, y representa a quantidade de um ativo y, e k é uma constante. A ideia é que o produto k dos ativos x e y deve permanecer constante de acordo com a fórmula definida. Se uma quantidade maior de ativos for adicionada ao pool de liquidez, então a constante mudará; no entanto, **enquanto houver negociações**, o efeito líquido manterá k constante. Em outras palavras, a fórmula de produto constante garante que o **preço dos ativos seja ajustado com base na oferta e na demanda**.

Por exemplo, a compra do ativo x **aumenta seu preço** e **diminui o preço** de y, e vice-versa. A razão entre o número de ativos x e y define o preço de forma correspondente. Esta fórmula garante que **haverá sempre liquidez**. Funções como **descoberta de preços**, **casamento de negociações** e **formação de mercado** são todas atendidas por esta fórmula simples.

**Vantagens dos AMMs**

Uma das principais vantagens dos AMMs é que eles **fornecem liquidez instantânea**, em vez de esperar por alguém que coloque uma ordem qualificada/adequada para atender à nossa troca. Em outras palavras, ele garante liquidez **mesmo na ausência de outros negociadores**, permitindo que compradores e vendedores troquem ativos com o pool de liquidez em vez de entre si.

Outra vantagem dos AMMs é que eles **diminuem a probabilidade de manipulação de preços**, como **negociação de lavagem (wash trading)** e **front running**, pois a fórmula codificada no contrato inteligente **mantém o valor dos pares de tokens constante**.

**Risco de Slippage (derrapagem)**

Existe, no entanto, o risco de **slippage**. *Slippage* pode ser definido como a **diferença entre o preço de mercado atual de um ativo e o preço pelo qual a ordem é executada**. No entanto, se o pool de liquidez tiver uma **liquidez profunda**, e os tamanhos das ordens forem menores, o slippage pode ser minimizado; contudo, ele **não é 100% evitável** nos CPMMs. O slippage pode ser **esperado ou inesperado**, e precisa ser gerenciado adequadamente.

Várias DEXs utilizam fórmulas de produto constante, incluindo **SushiSwap**, **Bancor** e várias outras.

**CSMM (Constant Sum Market Maker)**

Formadores de mercado de soma constante usam uma fórmula simples, conforme mostrado abaixo:

  x + y = k

A fórmula significa simplesmente que o formador de mercado manterá uma **soma fixa** dos dois ativos no pool. Embora essa seja uma função simples e ofereça **proteção contra slippage**, ela **não fornece liquidez ilimitada**.

**CMMM (Constant Mean Market Maker)**

Formadores de mercado de média constante possibilitam a criação de AMMs com **mais de dois tokens** e com **ponderações diferentes** da distribuição convencional 50/50. Nesta abordagem, a **média geométrica ponderada de cada reserva permanece inalterada**. Por exemplo, em um pool com três ativos, x, y e z, a fórmula seria:

  (x \* y \* z)^(1/3) = k

Esse atributo permite uma **exposição variável** a diferentes ativos no pool e **permite trocas entre quaisquer tokens do pool**.

**Comparação visual entre os modelos AMM**

Uma comparação em forma visual entre diferentes modelos de AMM é mostrada na **Figura 21.6** abaixo:

**<IMAGEM>**

Na figura acima, x, y e z são as quantidades dos ativos, com diferentes **relações matemáticas** entre eles conforme as fórmulas.

**DEX baseado em livro de ordens (Order book-based DEX)**

DEXs baseados em livro de ordens usam o **modelo tradicional de negociação**, que já existia muito antes do surgimento do DeFi. O modelo de livro de ordens, geralmente conhecido como **Livro de Ordens de Limite Central (CLOB – Central Limit Order Book)**, casa ordens de compra e venda de acordo com um conjunto de regras predeterminadas.

Em DEXs baseadas em livro de ordens, os operadores podem definir ordens de compra e venda para um ativo, e o livro de ordens organizará essas ordens com base em seus preços. Se houver **oferta e demanda** por um ativo, ele pode ser negociado nessas exchanges.

Exchanges baseadas em livro de ordens são adequadas para **mercados com alta liquidez**, pois conseguem **determinar com precisão os preços de mercado** e lidar com grandes ordens sem causar slippage significativo. Elas são preferidas tanto por **traders institucionais** quanto por **varejistas**, devido ao seu modelo de execução de negociações transparente e eficiente em termos de capital.

Existem dois tipos de DEXs baseadas em livro de ordens:

* **Livro de ordens on-chain**
* **Livro de ordens off-chain**

**Agregador de DEX (DEX Aggregator)**

Embora existam muitas plataformas DEX, cada uma possui **níveis diferentes de liquidez e preços**. Pode se tornar difícil para os usuários determinarem **qual DEX oferece o melhor preço e/ou liquidez**. É aqui que entram os **agregadores de DEX**. Como o nome sugere, os **agregadores de DEX** são plataformas onde a **liquidez de diferentes exchanges é agregada**. Em vez de acessar exchanges individuais, os usuários podem utilizar o agregador para negociar seus ativos.

A função de um agregador é encontrar:

* A **liquidez mais profunda**,
* Os **melhores preços**,
* As **menores taxas**,
* O **menor slippage**,
* E outros atributos ideais para o usuário, conforme suas exigências.

Existem dois tipos principais de agregadores em uso:

1. **Agregadores off-chain**
2. **Agregadores on-chain**

**Agregadores off-chain**

São geralmente implementados como **sites web** que fornecem o serviço de agregação.  
A principal **vantagem** desses agregadores é que normalmente estão **conectados com muitas blockchains**, são **muito flexíveis e eficientes**, e podem encontrar a **melhor estratégia para executar a negociação do usuário**.

O **ponto negativo**, no entanto, é que esses agregadores são **serviços centralizados**, ou seja, atuam como **terceiros confiáveis**. Isso pode levar a:

* **Front running de transações**,
* Seleção de estratégia **subótima**,
* E até **viés proposital** favorecendo uma exchange específica.

**Agregadores on-chain**

Como o nome sugere, são implementados **na própria blockchain**, e fornecem serviços de agregação por meio de um **contrato inteligente**. Esse contrato inteligente encontra uma **estratégia comprovadamente ótima de execução**, com:

* O melhor roteamento,
* Melhores lucros,
* E possibilidade de arbitragem.

Há também uma **probabilidade extremamente baixa de front running ou qualquer viés**, pois toda a lógica de agregação está **codificada em contratos inteligentes** rodando em uma **plataforma descentralizada**, ou seja, **on-chain**.

A **desvantagem** é que esses agregadores **não escalam bem** e geralmente conseguem cobrir apenas cerca de **três exchanges**.

**Limitações dos DEXs**

Algumas das limitações dos DEXs incluem:

* **Menor liquidez**,
* Funcionalidades mais limitadas do que exchanges centralizadas (por exemplo, ordens limitadas e de parada geralmente não estão disponíveis),
* **Interoperabilidade cross-chain muito limitada**, com a maioria das DEXs operando em **uma única blockchain** e raramente se comunicando com outras.

Apesar dessas limitações, o **ecossistema de DEXs está prosperando**, e essas limitações **não são grandes obstáculos à adoção e uso** dessas plataformas.

**Limitações dos AMMs**

Embora os AMMs ofereçam muitos benefícios, como liquidez contínua e acessibilidade, eles apresentam várias **limitações**. Algumas dessas limitações são descritas abaixo.

**Perda impermanente (Impermanent Loss)**

A **perda impermanente** ocorre quando o **preço dos ativos no pool de liquidez muda em relação ao preço em que foram depositados**, o que leva a um valor final **inferior ao que o provedor de liquidez teria se simplesmente tivesse mantido os ativos fora do pool**. Essa perda é chamada de **impermanente** porque pode desaparecer se o preço do ativo retornar ao valor original, mas se o provedor de liquidez retirar os fundos antes disso, a perda se torna **real/permanente**.

A perda impermanente é um dos maiores problemas nos AMMs com **modelo de produto constante (CPMM)**. O risco pode ser mitigado usando **mecanismos de hedge**, fornecendo **incentivos** aos provedores de liquidez ou utilizando **métodos de ajuste dinâmico da fórmula do AMM**.

**Baixa eficiência de capital**

Os AMMs também sofrem com **eficiência de capital limitada**, pois **os ativos no pool ficam ociosos a maior parte do tempo**, especialmente quando a negociação está concentrada em uma **faixa estreita de preços**. Isso significa que **grande parte do capital não está sendo usada efetivamente**, o que representa uma ineficiência do sistema.

Algumas abordagens tentam resolver esse problema permitindo que os **provedores de liquidez concentrem sua liquidez em determinadas faixas de preço** (por exemplo, **Uniswap v3**). Isso melhora a **eficiência do capital**, pois mais liquidez é usada dentro da faixa onde ocorre a maioria das negociações.

**Propostas para superar essas limitações**

Várias soluções têm sido propostas para resolver as limitações mencionadas anteriormente. Algumas das mais promissoras incluem:

* **AMMs híbridos** que combinam o modelo AMM com **livros de ordens**, oferecendo o melhor dos dois mundos.
* **Formadores de mercado proativos (Proactive Market Makers)** que ajustam automaticamente os preços com base em modelos preditivos ou sinais externos.
* **AMMs baseados em curvas customizadas**, como os usados em protocolos como **Curve Finance**, que são otimizados para negociação de ativos similares, como **stablecoins**.
* **AMMs com elasticidade dinâmica**, que ajustam dinamicamente os parâmetros do modelo para reduzir o slippage e a perda impermanente.
* **Modelos de market making programáveis**, que permitem aos provedores de liquidez **definir suas próprias curvas de precificação** personalizadas.

**Plataformas de empréstimos (Lending Platforms)**

O empréstimo de ativos cripto no DeFi é muito comum. O modelo tradicional exige que um credor (como um banco) empreste ativos a um mutuário (como uma pessoa ou empresa). O mutuário paga **juros ao credor**, e a quantia principal é reembolsada no final do período de empréstimo. A **taxa de juros** depende da **qualidade de crédito do mutuário**, garantias e outros fatores. A principal limitação é que o empréstimo é frequentemente **inacessível para muitas pessoas** devido à complexidade, pontuações de crédito, requisitos regulatórios e outros entraves.

As **plataformas DeFi de empréstimos** buscam resolver esses problemas fornecendo um sistema **aberto, sem permissão, sem confiança e transparente** onde **qualquer pessoa pode emprestar ou tomar emprestado ativos**. Essas plataformas funcionam com base em **contratos inteligentes**, que eliminam intermediários, reduzindo custos e aumentando a eficiência.

O funcionamento de uma plataforma de empréstimo DeFi é o seguinte:

1. **Usuários depositam ativos no protocolo** (por exemplo, ETH, USDC, DAI etc.). Esses ativos formam o **pool de liquidez** do qual outros usuários podem tomar emprestado.
2. Um usuário que deseja tomar emprestado precisa **bloquear colateral** – geralmente em cripto – que é **supercolateralizado** (ou seja, o valor do colateral é maior do que o valor tomado emprestado).
3. O contrato inteligente **determina a taxa de juros** com base na **oferta e demanda** dos ativos no pool.
4. Se o valor do colateral cair abaixo de um determinado limite (índice de liquidação), o contrato inteligente **liquida automaticamente** a posição do mutuário para proteger o pool.
5. Os credores recebem **juros sobre seus depósitos** à medida que os mutuários pagam seus empréstimos.

**Exemplos de plataformas de empréstimo DeFi**

* **Aave**: Protocolo não custodial de empréstimos que permite aos usuários emprestar e tomar emprestado criptoativos.
* **Compound**: Plataforma de taxas de juros algorítmicas baseada em Ethereum.
* **MakerDAO**: Permite a geração de DAI (uma stablecoin) ao bloquear colateral.
* **Cream Finance**, **Venus**, entre outros.

**Vantagens das plataformas DeFi de empréstimos**

* **Acessibilidade global**: qualquer pessoa com acesso à internet pode usar a plataforma.
* **Sem necessidade de pontuação de crédito**: as garantias fornecem segurança.
* **Transparência**: os contratos inteligentes e suas regras são públicos.
* **Eficiência**: sem intermediários, reduzindo custos e tempo.

**Riscos envolvidos**

* **Risco de liquidação**: devido à volatilidade dos ativos, o valor do colateral pode cair repentinamente.
* **Risco de contrato inteligente**: bugs ou vulnerabilidades podem ser explorados.
* **Risco de oráculo**: dados incorretos podem afetar as avaliações de colateral.
* **Risco sistêmico**: falha em um grande protocolo pode causar efeito cascata em outros.

**Seguros**

O setor de seguros no DeFi tem crescido significativamente. A natureza **sem confiança**, **descentralizada** e **transparente** das plataformas DeFi também permite a criação de **seguros descentralizados**. O conceito é simples:  
Em vez de depender de uma seguradora centralizada tradicional, o seguro pode ser fornecido por meio de **contratos inteligentes**, onde **provedores de liquidez** contribuem com ativos para um **pool de seguro**, e os **usuários compram apólices** (geralmente também tokens) para **se proteger contra riscos específicos**.

Esses riscos podem incluir:

* Risco de falha do contrato inteligente
* Risco de oráculo
* Risco de ataque de hackers
* Risco de slashing em staking
* E outros eventos inesperados

O processo geralmente envolve o seguinte:

1. Um usuário compra cobertura pagando um **prêmio**.
2. Os fundos do prêmio são adicionados ao pool.
3. Se ocorrer um evento coberto, o usuário envia uma **reivindicação**.
4. A reivindicação é avaliada pela comunidade ou por um contrato inteligente.
5. Se aprovada, o pagamento é realizado automaticamente.

Alguns projetos de seguro DeFi incluem:

* **Nexus Mutual**
* **Etherisc**
* **InsurAce**
* **Bridge Mutual**

A descentralização no setor de seguros permite **maior transparência**, **menor custo** e **cobertura personalizada**, embora ainda haja desafios relacionados à **avaliação precisa de riscos** e **prevenção de fraudes**.

**Ativos sintéticos**

Um **ativo sintético** é um instrumento financeiro construído para **imitar o comportamento de outro ativo**. Em outras palavras, trata-se de **um derivativo tokenizado** que representa o valor de um ativo real, como:

* Ações
* Moedas fiduciárias
* Commodities
* Índices
* E até outros criptoativos

Esses ativos permitem que os usuários obtenham **exposição a ativos tradicionais sem realmente possuí-los**, apenas mantendo o token sintético.

Os contratos inteligentes garantem que o ativo sintético permaneça **indexado ao preço real** por meio de **oráculos**, **colateralização** e **mecanismos de incentivo**. Os ativos sintéticos são particularmente poderosos porque:

* Expandem o alcance do DeFi para ativos fora da blockchain
* Permitem diversificação e alavancagem
* Podem ser usados por qualquer pessoa, em qualquer lugar, sem restrições

Plataformas populares de ativos sintéticos incluem:

* **Synthetix**
* **Mirror Protocol**
* **UMA (Universal Market Access)**

**Derivativos**

**Derivativos** são contratos financeiros cujo valor depende de outro ativo — o **ativo subjacente**. No DeFi, derivativos são **implementados como contratos inteligentes** que permitem a criação e negociação de produtos complexos, como:

* Futuros
* Opções
* Swaps
* Contratos perpétuos

Esses produtos permitem aos traders:

* Fazer hedge contra risco
* Alavancar posições
* Apostar na direção do mercado

Plataformas populares de derivativos DeFi incluem:

* **dYdX**
* **Perpetual Protocol**
* **Hegic**
* **Opyn**

**Governança no DeFi**

A governança é um componente essencial no DeFi, pois define **como decisões são tomadas** dentro de um protocolo descentralizado. Em vez de depender de um conselho ou diretoria central, os projetos DeFi geralmente utilizam **modelos de governança descentralizada**, baseados em:

* **Tokens de governança**
* **Mecanismos de votação on-chain**
* **Propostas submetidas pela comunidade**

Os **tokens de governança** conferem aos seus detentores **o direito de propor, votar e aprovar alterações** no protocolo, tais como:

* Atualizações técnicas
* Parâmetros do protocolo (como taxas de juros, limites de colateralização)
* Distribuição de fundos do tesouro
* Parcerias e listagens

Esse modelo **democratiza o controle** da plataforma e promove **maior alinhamento com os interesses dos usuários**, mas também pode gerar riscos de **governança capturada** (por baleias ou grandes detentores de tokens) e **baixo engajamento** da comunidade.

**DAOs (Organizações Autônomas Descentralizadas)**

As DAOs são o **mecanismo organizacional fundamental** por trás da governança DeFi. Uma DAO é uma entidade totalmente **baseada em código**, sem liderança central, que é:

* **Regida por contratos inteligentes**
* **Controlada por participantes através de votos**
* **Totalmente transparente**, pois tudo é registrado na blockchain

Funções típicas de uma DAO incluem:

* **Gerenciamento de tesouro** (fundos do protocolo)
* **Administração de atualizações do protocolo**
* **Revisão e votação de propostas da comunidade**
* **Concessão de fundos para desenvolvedores, pesquisas ou marketing**

Exemplos populares de DAOs incluem:

* **MakerDAO**
* **Compound Governance**
* **Uniswap DAO**
* **Aave Governance**

As DAOs representam um novo modelo de **colaboração sem fronteiras**, em que **qualquer pessoa pode participar e contribuir**, desde que siga as regras programadas no código.

**Considerações finais**

O ecossistema DeFi representa uma **evolução significativa dos serviços financeiros** tradicionais. Ele oferece:

* Acessibilidade global
* Maior eficiência
* Redução de custos
* Inclusão financeira
* Transparência e auditabilidade
* Resistência à censura

No entanto, o DeFi também **não está isento de riscos**. Alguns dos principais desafios incluem:

* **Riscos de segurança** em contratos inteligentes e oráculos
* **Volatilidade** dos ativos digitais
* **Problemas regulatórios** ainda indefinidos
* **Falta de proteção ao consumidor**
* **Riscos de governança mal estruturada**
* **Possibilidade de exploits e manipulações de mercado**

Apesar desses desafios, o DeFi está **crescendo exponencialmente** e se expandindo para novas áreas como:

* **DeSci (Decentralized Science)**
* **ReFi (Regenerative Finance)**
* **DeGov (Governança descentralizada)**
* **GameFi (Finanças em jogos)**
* **NFT-Fi (Finanças com NFTs)**

Com o tempo, espera-se que o DeFi **amadureça** e **se integre com o sistema financeiro tradicional**, criando uma nova infraestrutura **híbrida e inclusiva**, com potencial de **redefinir o conceito de finanças para as próximas gerações**.