**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.

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:

****

***Figure 21.1: Trade lifecycle***

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.

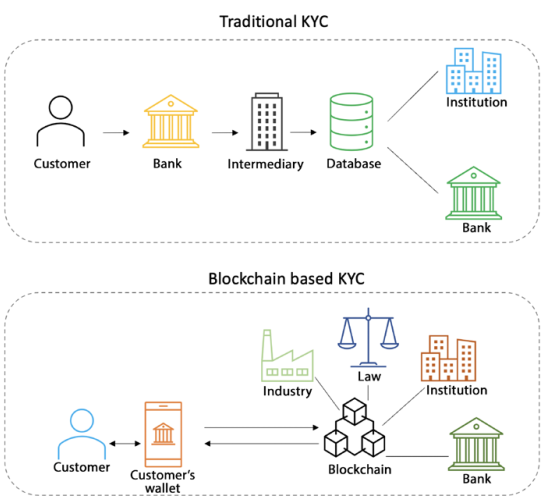
No modelo tradicional de ciclo de vida da negociação, uma **câmara de compensação central** é necessária para facilitar a negociação entre as partes, que assume o risco de crédito de ambas as partes. O esquema atual é um tanto complicado, no qual um vendedor e um comprador devem seguir uma rota complicada 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:

****

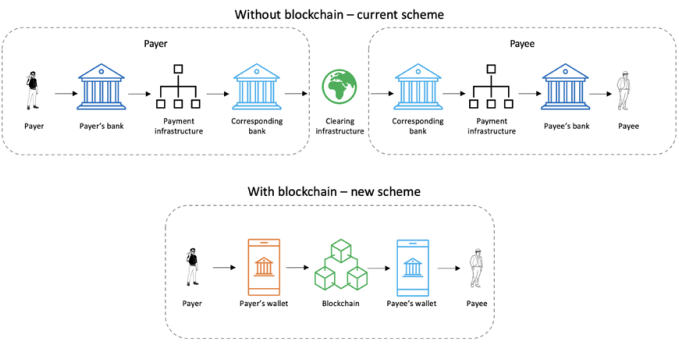
***Figure 21.2: Traditional vs blockchain-based KYC***

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.

****

***Figure 21.3: Cross-border payment system – from complex to simple using blockchain***

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:**

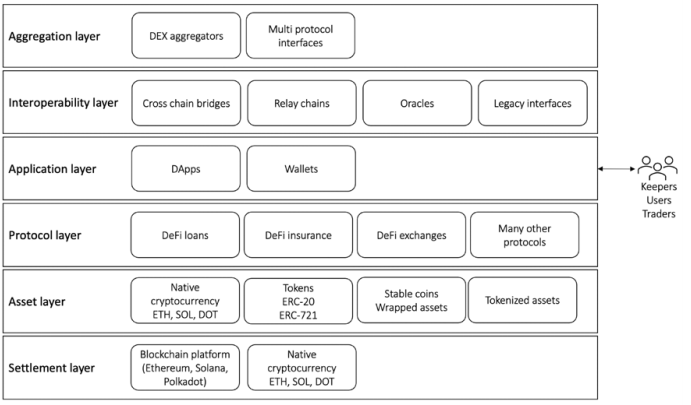
**Camadas do DeFi**

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:

****

***Figure 21.4: DeFi layered architecture***

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, componentes e serviços diferentes. Discutimos esses serviços a seguir.

**Tokenização de ativos**

Esta é a base sobre a qual o DeFi é construído. É o 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. Por exemplo, tokenizar uma obra de arte famosa.

Trocadores descentralizados

Podemos dividir os trocadores (exchanges) em dois tipos: trocadores centralizados e trocadores descentralizados.

Um trocador é tradicionalmente centralizado, o que significa que alguns deles podem não ser totalmente confiáveis. Eles não são transparentes, e a custódia também é centralizada. Vimos como trocadores de criptomoedas centralizados foram alvo de hacks e más práticas e, como resultado, bilhões de fundos foram perdidos. Por exemplo, Mt. Gox, Coincheck e Binance sofreram perdas devido a ataques de hackers bem-sucedidos no passado.

Um trocador descentralizado (DEX) alivia os problemas enfrentados por um trocador centralizado (CEX). Podemos definir um DEX como um tipo de trocador 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 os trocadores centralizados, que atuam como intermediários e como custodiante dos ativos dos seus usuários.

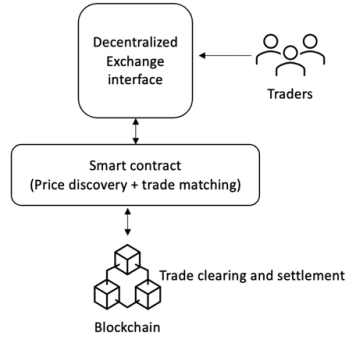
No DeFi e em sistemas de negociação baseados em blockchain em geral, a negociação de tokens é a atividade principal. Tokens podem ser negociados em trocadores. Com o advento do DeFi, surgiram os trocadores descentralizados. DEXs são descentralizados e, portanto, não exigem autoridade central ou intermediário para facilitar a negociação. DEXs são descentralizados, transparentes e não custodiais.

Embora a barreira de entrada para os DEXs seja baixa devido à ausência de exigências regulatórias tradicionais, como os requisitos de KYC, isso também os torna arriscados para os investidores, pois, se por algum motivo o DEX for hackeado, não há proteção contra perda de fundos. KYC é uma prática padrão de due diligence na indústria de serviços financeiros que garante que o cliente seja legítimo e genuíno. No entanto, algumas exchanges cripto centralizadas agora começaram a fazer verificações de KYC e AML.

Alguns exemplos de DEXs são Uniswap, Bancor, WavesDEX, 0x e IDEX. Este ecossistema está crescendo a um ritmo muito acelerado e espera-se que continue crescendo.

**Finanças descentralizadas**

A estrutura básica de um DEX é composta por um contrato inteligente que facilita a negociação entre duas partes. Este contrato inteligente consiste em três funções: descoberta de preço, correspondência de negociação e liquidação de negociação. Podemos visualizar isso na Figura 21.5 abaixo:



*Figure 21.5: High-level architecture of a DEX*

**Descoberta de preço** é o processo de determinar o valor justo de mercado de um ativo financeiro por meio das forças de oferta e demanda no mercado. Isso 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 preço ocorre por meio de vários mecanismos, como negociações em exchanges, transações OTC e o 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.

Existem vários tipos de DEXs, incluindo AMM (também chamado de DEX baseado em pool de liquidez), DEX baseado em livro de ordens e agregador de DEX. A classificação é mostrada abaixo:

1. Market Maker Automatizado:

a. Livro de ordens on-chain  
b. Livro de ordens off-chain

1. Agregadores de DEX

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

Qualquer trader que utilize o pool de liquidez para trocar ativos paga uma taxa ao usuário que forneceu liquidez ao adicionar seus tokens ao pool de liquidez. A ideia central por trás do AMM é permitir que contratos inteligentes façam a criação de mercado, em vez de os usuários colocarem ordens manualmente. Em resumo, os pools de liquidez podem ser considerados como “potes” compartilhados de fundos usados pelos DEXs e depositados pelos usuários do DEX, conhecidos como provedores de liquidez. Pools de liquidez são usados pelos DEXs para comprar, vender e cumprir ordens. Provedores de liquidez ganham taxas do pool em troca de manter os fundos bloqueados no pool, por meio de um processo chamado mineração de liquidez.

Existem vários modelos de AMM. AMMs usam fórmulas matemáticas para ajustar os preços no pool de liquidez. Essa fórmula matemática é programada no contrato inteligente. Existem vários modelos de criadores de mercado de função constante, incluindo CPMM, CSMM e CMMM.

**CPMM**  
A fórmula de criador de mercado de produto constante é simplesmente o produto de dois ativos, conforme mostrado na equação abaixo:  
𝑥 \* 𝑦 = 𝑘

Onde x representa a quantidade de algum ativo x, y representa a quantidade de algum ativo y, e k é uma constante. A ideia é que o produto k dos ativos x e y deve permanecer constante conforme uma constante definida. Se uma quantidade maior de ativos for adicionada ao pool de liquidez, então a constante mudará; no entanto, enquanto forem negociados, o efeito líquido manterá k constante. Em outras palavras, a fórmula de produto constante garante que o preço dos ativos seja ajustado conforme a oferta e a demanda. Por exemplo, a compra do ativo x aumenta o preço de x e diminui o preço de y, e vice-versa. A proporção do número de ativos x e y define o preço conforme. Essa fórmula de produto constante garante que a liquidez esteja sempre disponível. Funções como descoberta de preço, correspondência de negociação e criação de mercado são todas atendidas por essa fórmula simples.

Um dos principais benefícios dos AMMs é que eles fornecem liquidez instantânea, em vez de esperar que alguém coloque uma ordem qualificada/apropriada para cumprir uma troca. Em outras palavras, garante liquidez mesmo na ausência de outros traders, permitindo que compradores e vendedores troquem ativos com o pool de liquidez em vez de entre si. Outra vantagem do AMM é que ele diminui a probabilidade de táticas de manipulação de preços, como negociação fictícia (wash trading) e front running, pois a fórmula codificada no contrato inteligente mantém o valor dos pares de tokens constante.

No entanto, há o risco de *slippage* (deslizamento). *Slippage* pode ser definido como a diferença entre o preço de mercado atual de um ativo e o preço no qual a ordem é executada. No entanto, se o pool de liquidez tiver liquidez profunda, e os tamanhos das ordens também forem menores, o *slippage* pode ser minimizado; entretanto, não é 100% evitável em CPMMs. O *slippage* pode ser esperado ou inesperado e precisa ser gerenciado de acordo.

Vários DEXs utilizam fórmulas de produto constante, incluindo SushiSwap, Bancor e vários outros.

**CSMM**

Criadores de mercado de soma constante utilizam uma fórmula simples como mostrada abaixo:

**x + y = k**

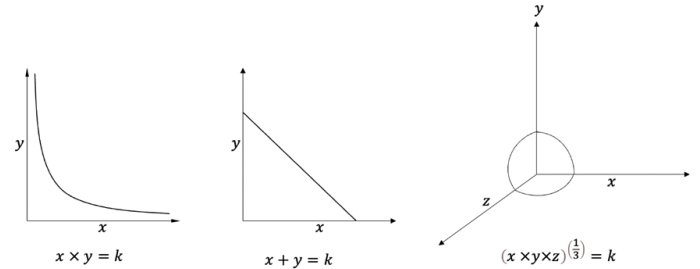
A fórmula simplesmente significa que o criador de mercado manteria uma soma fixa dos dois ativos no pool. Embora essa seja uma função simples e ofereça proteção contra *slippage*, ela não fornece liquidez ilimitada.

**CMMM**

Criadores de mercado de média constante facilitam a formação de AMMs com mais de dois tokens e ponderações que diferem da distribuição convencional de 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 exposição variável a diferentes ativos no pool e permite trocas entre quaisquer dos tokens do pool.

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



*Figure 21.6: CPMM vs CSMM vs CMMM*

No diagrama anterior, x, y e z são as quantidades dos ativos, com diferentes relações matemáticas entre eles conforme a fórmula.

**DEX baseado em livro de ordens**

DEXs baseados em livro de ordens utilizam o modelo tradicional de negociação, que existe há muito tempo antes do surgimento do DeFi. O modelo de livro de ordens, geralmente conhecido como Livro de Ordens com Limite Central (CLOB), corresponde ordens de compradores e vendedores de acordo com um conjunto de regras predefinidas. Em DEXs baseados em livro de ordens, os traders podem definir ordens de compra e venda para um ativo, e o livro de ordens as organizará com base em seus preços. Se houver oferta e demanda para um ativo, ele pode ser negociado nessas exchanges. Exchanges de livro de ordens são adequadas para mercados com alta liquidez, pois podem determinar preços de mercado com precisão e lidar com grandes ordens sem *slippage* significativo. São preferidas por traders institucionais e de varejo devido ao seu modelo de execução de negociação eficiente em capital e transparente. Existem dois tipos de DEXs baseados em livro de ordens: livro de ordens *on-chain* e livro de ordens *off-chain*.

**Capítulo 21**

**Agregador de DEX**

Embora existam muitas plataformas de DEX, cada uma possui diferentes níveis de liquidez e preços. Pode ser difícil para os usuários descobrir qual DEX oferece o melhor preço e/ou liquidez. É aqui que os agregadores de DEX podem ajudar. Agregadores de DEX, como o nome sugere, são plataformas onde a liquidez de diferentes exchanges é agregada. Em vez de ir para DEXs individuais, os usuários podem usar o agregador para negociar seus ativos. O trabalho de um agregador é encontrar a liquidez mais profunda, os melhores preços, as menores taxas, o menor *slippage* e outros atributos mais adequados para o usuário de acordo com seus requisitos.

Existem dois tipos desses agregadores comumente em uso: agregadores *off-chain* e agregadores *on-chain*. Agregadores *off-chain* geralmente são implementados como sites que fornecem o serviço de agregação. A principal vantagem de tal agregador é que eles geralmente estão conectados a muitas blockchains, são muito flexíveis e eficientes, e podem encontrar a estratégia ideal para executar a negociação para os usuários. A desvantagem, no entanto, é que esses agregadores são efetivamente terceiros confiáveis, e esses são serviços centralizados, o que pode levar a *front running*, seleção de estratégias subótimas e até mesmo seleção de estratégias enviesadas que podem favorecer uma exchange específica.

Agregadores *on-chain*, como o nome sugere, rodam em uma blockchain, e fornecem serviços de agregação usando um contrato inteligente. Este contrato inteligente encontra uma estratégia comprovadamente ótima para execução com o melhor roteamento, melhores lucros e possibilidade de arbitragem. Também há uma probabilidade extremamente baixa de *front running* ou qualquer viés, devido a toda a lógica de agregação estar codificada nos contratos inteligentes que rodam em uma plataforma descentralizada, ou seja, *on-chain*. Embora isso seja uma vantagem, uma desvantagem importante é que esses agregadores não escalam bem e geralmente cobrem apenas cerca de três exchanges.

Algumas limitações dos DEX incluem menor liquidez, recursos comparativamente limitados em relação às exchanges centralizadas (nas quais recursos como ordens limitadas, ordens de parada etc. estão disponíveis, mas tais recursos não estão disponíveis nos DEXs) e interoperabilidade entre cadeias muito limitada, em que a maioria dos DEXs realmente opera apenas em uma cadeia e raramente interage com outras. No entanto, o ecossistema DEX está prosperando, e essas limitações não são um grande obstáculo à adoção e uso dos DEXs. Especificamente, nos modelos AMM, perda impermanente e baixa eficiência de capital são duas limitações principais.

**Perda impermanente** ocorre quando o valor dos ativos que você depositou em um pool de liquidez flutua, ou seja, aumenta ou diminui em comparação com o valor quando você os depositou. Isso significa que o valor dos ativos depositados pode ser diferente quando forem retirados em comparação com quando foram inicialmente depositados no pool. Vale notar que o termo “impermanente” pode ser enganoso, já que uma queda no preço de um token pode ser apenas temporária e pode subir novamente devido a condições de mercado ou outros fatores. Neste caso, a perda seria considerada temporária, ou impermanente, porque o preço eventualmente voltou a subir. No entanto, se o valor em dólares (valor gerado após a conversão do ativo cripto em USD) do token no momento da retirada for menor do que o valor quando foi depositado, então a perda torna-se permanente.

AMMs também precisam de uma grande quantidade de liquidez para igualar o impacto de precificação de uma exchange baseada em livro de ordens, o que resulta em baixa eficiência de capital.

Para lidar com essas limitações, várias inovações foram propostas, incluindo *market makers* automáticos dinâmicos, *market makers* híbridos de função constante, *market makers* proativos e *market makers* automáticos virtuais.

Um modelo **DAMM** pode usar alimentações de preço através de oráculos e volatilidade implícita para distribuir a liquidez de forma mais eficaz ao longo da curva de preços. O modelo pode criar um *market maker* mais resiliente que pode se adaptar às mudanças nas condições de mercado ao integrar várias variáveis dinâmicas no algoritmo. Quando a volatilidade está baixa, o modelo pode concentrar liquidez perto do preço de mercado para melhorar a eficiência de capital, o que pode ser estendido durante períodos de alta volatilidade para proteger os traders contra perda impermanente. Em termos simples, a relação matemática (por exemplo, 𝑥 \* 𝑦 = 𝑘) entre os ativos é ajustada dinamicamente para garantir que o preço do pool se alinhe continuamente e automaticamente com o preço de mercado. Essa técnica visa eliminar oportunidades de arbitragem.

**Market Makers Híbridos de Função Constante (CFMMs)** combinam várias propriedades dos AMMs, funções e parâmetros para alcançar um mecanismo mais estável, eficiente e lucrativo para os traders.

**AMMs virtuais** visam minimizar o impacto de preço e mitigar a perda impermanente. Eles usam a mesma fórmula de produto constante que os AMMs tradicionais — isto é, 𝑥 \* 𝑦 = 𝑘 — mas em vez de confiar em um pool de liquidez, os traders depositam colateral em um contrato inteligente. Isso permite negociar ativos sintéticos em vez do ativo subjacente, o que permite que os usuários tenham exposição ao movimento de preço de muitos ativos cripto de forma eficiente.

O modelo **Market Maker Proativo (PMM)** foi desenvolvido para aumentar a liquidez nos protocolos. Este modelo imita o comportamento de um *market maker* humano em um livro de ordens centralizado tradicional usando preços de mercado precisos provenientes de um oráculo. Em resposta às mudanças do mercado, o protocolo PMM move proativamente a curva de preço de um ativo, aumentando a liquidez perto do preço de mercado atual. Isso facilita a negociação eficiente e reduz a perda impermanente para os provedores de liquidez.

Outro problema de que os AMMs sofrem é o **front running**. Isso ocorre quando outro usuário realiza uma negociação semelhante à de um comprador potencial, mas a executa rapidamente e vende de volta, fazendo com que o preço suba, e então lucra com o aumento do preço. Isso é possível porque as transações nos AMMs são públicas. Também conhecido como **ataque sanduíche**, isso é frequentemente automatizado usando bots, o que agrava a situação. Em muitos casos, os mineradores são os responsáveis pelo front running, o que levou ao termo **Miner Extractable Value (MEV)**, referindo-se aos lucros injustos que um terceiro pode obter com a transação original.

**Prós e contras dos AMMs**

Uma das principais vantagens dos AMMs é que não é necessário manter um livro de ordens. As fórmulas relacionadas ao produto constante (CP) são simplesmente implementáveis em contratos inteligentes. No entanto, algumas desvantagens incluem o risco de perda impermanente, alto *slippage* (deslizamento), e outros riscos tecnológicos de segurança, que serão abordados no Capítulo 19, **Segurança em Blockchain**.

**CEX vs DEX**

Uma comparação entre CEX e DEX é apresentada abaixo e destaca as principais diferenças entre os dois paradigmas:

| **Atributo / tipo de exchange** | **CEX** | **DEX** |
| --- | --- | --- |
| Custódia de ativos | Terceiros | Usuário |
| Barreira de entrada | Alta | Muito baixa |
| Regulação | Alta | Nenhuma, ou muito baixa |
| Disponibilidade de infraestrutura | Alta (mas pode ser comprometida devido à centralização) | Muito alta (devido às garantias de segurança da blockchain) |
| Experiência do usuário | Fácil de usar; com suporte | Pode ser difícil de usar para novos usuários; menos suporte |
| Liquidez | Muito mais profunda e fornecida profissionalmente | Não muito profunda |
| Perda impermanente | Não aplicável, pois é altamente líquido | Aplicável e muito provável em caso de flutuações |
| Taxas | Mais altas, devido a intermediários | Muito mais baixas, pois não há intermediários |
| Verificação de identidade | Necessária | Não necessária |

Como o DeFi é um ecossistema em expansão com enormes oportunidades de lucro, surge a seguinte pergunta: é possível encontrar automaticamente a estratégia de negociação mais lucrativa e criar negociações DeFi de acordo para maximizar os lucros? Existem dois métodos empregados para isso – o **algoritmo de Bellman-Ford** e os **solucionadores SMT**.

**Empréstimos instantâneos (Flash loans)**

Um *flash loan* é um serviço que existe apenas no mundo DeFi. No CeFi, um empréstimo é um instrumento que se refere a um acordo entre um credor e um tomador, no qual o tomador recebe uma certa quantia de fundos (o empréstimo) do credor, com a obrigação de reembolsar o valor do empréstimo mais os juros durante um período especificado. Os instrumentos de empréstimo normalmente envolvem o pagamento de juros e principal regularmente, e são garantidos ou não garantidos. Empréstimos garantidos são respaldados por algum tipo de colateral, como uma propriedade ou um veículo, enquanto empréstimos não garantidos não possuem garantia e geralmente são oferecidos a uma taxa de juros mais alta. O credor assume o risco de inadimplência e é compensado pela taxa de juros cobrada durante o período do empréstimo. Se o empréstimo for de longa duração, então a taxa de juros também é maior porque há maior exposição ao risco de inadimplência por parte do tomador em razão do período mais longo. Isso significa que se o empréstimo for de curto prazo, então o risco é menor e, portanto, exige menos compensação para o credor.

Um *flash loan* permite tais empréstimos de curto prazo, que são instantâneos e pagos de volta na mesma transação. Em outras palavras, o reembolso do empréstimo ocorre na mesma transação em que o empréstimo foi concedido. *Flash loans* são atômicos por natureza devido à blockchain subjacente, significando que se o empréstimo (principal) não for reembolsado com os juros exigidos dentro da mesma transação, todo o processo retorna ao estado anterior como se nenhum dinheiro jamais tivesse saído da conta do credor. Isso significa que não há risco de contraparte ou de duração nos *flash loans*, o que é totalmente diferente dos empréstimos no mundo financeiro tradicional.

Essa condição de segurança é imposta via transações atômicas habilitadas por blockchain. As operações dentro de uma transação são executadas completamente em ordem sequencial ou falham por completo. Uma transação blockchain pode falhar por três razões: taxas de transação insuficientes, a transação (chamada de função) falha em atender às condições no contrato inteligente, ou a transação é ilícita (por exemplo, tentativa de gasto duplo). Em todos esses casos, o estado será revertido automaticamente ao estado anterior como se nenhuma transação jamais tivesse sido executada. Esse mecanismo de segurança inerente permite os *flash loans*.

Se um usuário pegar emprestado um milhão de dólares em tokens e falhar em atender às condições do empréstimo estabelecidas no contrato inteligente (por exemplo, reembolsá-lo até o final da transação com os juros), a transação será revertida devido à segurança inerente do mecanismo de execução de transações blockchain. Imagine que dentro de uma única transação, o empréstimo é emitido a partir do *pool* de liquidez, o empréstimo é usado, e o valor principal com juros é reembolsado ao *pool* de liquidez. Imagine se a última condição não for atendida, ou seja, o empréstimo e os juros não forem pagos — a transação inteira do *flash loan* falha e nenhuma mudança de estado ocorre, como se nenhum empréstimo tivesse sido emitido. Essa segurança garante ao credor que o empréstimo será sempre pago; caso contrário, nenhum empréstimo será emitido. Em segundo lugar, não há limite para a quantia que o tomador pode solicitar, dado que há fundos suficientes disponíveis no *pool*. Isso é extremamente poderoso, e nenhuma estrutura similar existe (ou pode existir) nas finanças tradicionais.

*Flash loans* são **não colateralizados**, o que significa que permitem a um usuário aproveitar oportunidades de arbitragem (diferença de preços) ou refinanciar sem precisar empenhar qualquer ativo como garantia. *Flash loans* são acessíveis a qualquer pessoa; tudo o que é necessário é uma carteira e a quantia requerida de fundos, independentemente de sua solvência ou status financeiro. Isso, novamente, contrasta fortemente com os instrumentos de empréstimo nas finanças tradicionais e permite que qualquer pessoa tenha acesso a possibilidades que antes não eram possíveis no mundo CeFi. *Flash loans* oferecem **arbitragem sem risco**. Em resumo, não existe nenhum análogo de *flash loans* nas finanças tradicionais.

Alguns exemplos de provedores de *flash loans* incluem [Equalizer](https://equalizer.finance) e [Aave](https://aave.com).

**Derivativos**

Derivativos no mundo DeFi servem ao mesmo propósito dos derivativos nas finanças tradicionais, ou seja, **proteger contra risco de preço** e **interagir com um ativo específico sem comprá-lo**. O valor dos derivativos DeFi é geralmente derivado de mercados de criptomoedas, mas também pode estar vinculado a outros ativos tradicionais como commodities e moedas fiduciárias. Protocolos de derivativos DeFi permitem que os usuários criem ativos sintéticos que estão atrelados a algum ativo real subjacente. Alguns exemplos de protocolos de derivativos DeFi são:

* [Synthetix](https://synthetix.io)
* [Hegic](https://www.hegic.co)
* [Opyn](https://www.opyn.co)

Esses protocolos permitem que investidores negociem derivativos ligados a diversos ativos subjacentes, como commodities, criptomoedas e índices.

Existem dois tipos de derivativos descentralizados: derivativos **baseados em ativos** e **baseados em eventos**. Derivativos baseados em ativos são oferecidos por serviços como Synthetix e Mirror, enquanto derivativos baseados em eventos são oferecidos por serviços como Augur.

Derivativos baseados em ativos têm seu valor atrelado ao valor de um ativo subjacente, que pode ser uma criptomoeda importante como Bitcoin, Ethereum ou qualquer outro ativo financeiro. Enquanto o ativo subjacente em derivativos garantidos por ativos é sempre financeiro, no caso dos derivativos baseados em eventos, o ativo subjacente é algum evento, ou seja, uma variável observável. Nestes mercados, indivíduos fazem apostas sobre o resultado de eventos como jogos, eleições, entre outros.

**Transmissão de dinheiro (*Money streaming*)**

Pagamentos descentralizados já são uma norma no mundo DeFi; entretanto, e se pudéssemos torná-los ainda mais baratos, rápidos, programáveis, condicionais, baseados em tempo, em tempo real e mais flexíveis?

O conceito de **pagamentos em fluxo contínuo (streaming)** surgiu no DeFi, o que significa que, em vez de esperar por um período fixo tradicional (por exemplo, semanal ou mensal) para pagamento, os pagadores podem “transmitir” pagamentos em tempo real, em pequenos incrementos, assim como transmitimos vídeos online. Os fundos podem ser transmitidos em intervalos acordados entre as partes envolvidas. Uma plataforma que permite isso é a **Sablier**, que permite a transmissão de tokens em intervalos regulares. Uma das principais vantagens dos pagamentos contínuos é que os beneficiários podem verificar que estão sendo pagos **agora**, em vez de esperar e confiar que o pagador irá pagar em uma data e hora futuras específicas.

Além disso, ao receber um salário em tempo real, o conceito de “dia de pagamento” é eliminado, o que leva a uma redução significativa na necessidade de empréstimos de adiantamento salarial. Esse método permite que os indivíduos verifiquem que estão sendo pagos imediatamente e regularmente nos intervalos de tempo que são adequados para eles, em vez de depender da promessa de pagamento futuro. Empresas também podem evitar desperdiçar uma quantia considerável de dinheiro com contabilidade, faturamento e registros de data e hora, porque o processo de transmissão de dinheiro pode ser mais eficiente e eliminar as necessidades contábeis tradicionais. Outra ideia poderia ser **faturamento em fluxo (stream billing)**, onde as contas são pagas em intervalos mais frequentes e curtos em tempo real, o que pode aliviar o problema de pagar todas as contas mensalmente de uma só vez. Termos semelhantes como **finanças em tempo real**, **transmissão de tokens** e **dinheiro social** têm surgido na literatura, que fundamentalmente significam a mesma coisa – a capacidade de realizar pagamentos em tempo real e de forma flexível.

***Yield farming***

*Yield farming* é um método popular para gerar renda passiva por parte de traders. Esses protocolos de *yield farming* são programados usando contratos inteligentes. Contratos inteligentes protegem os tokens dos usuários/traders e oferecem juros sobre os ativos bloqueados. Se esses tokens bloqueados forem usados para fornecer liquidez, os traders podem ganhar juros com base nas taxas de transação. A liquidez geralmente é necessária para que os DEXs facilitem a negociação. Como esses tokens bloqueados podem ser usados nos DEXs para executar ordens de compra e venda, os *yield farmers* podem obter renda por meio de taxas de transação. Além disso, se os tokens bloqueados forem usados para empréstimos, os investidores podem receber juros de empréstimo.

Os juros pagos aos traders podem equilibrar os riscos potenciais de bloquear seus tokens, tais como **perda impermanente**, **volatilidade dos tokens** e o risco de **“rug pulls”** (quando os desenvolvedores abandonam um projeto levando os fundos). A **taxa percentual anual (APR)** pode ser decidida pelo criador do *pool* ou automaticamente determinada pelo protocolo de *yield farming*, cuja lógica está codificada nos contratos inteligentes que implementam o protocolo na blockchain.

**Seguro**

Discutimos anteriormente alguns casos de uso de seguros neste capítulo, no contexto de casos de uso da blockchain em finanças. Esses casos de uso estão relacionados ao fornecimento e à melhoria de produtos de seguros que existem no mundo financeiro tradicional. Por exemplo, um caso em que as condições climáticas monitoradas por um sensor IoT em uma área agrícola disparam automaticamente um pagamento de seguro via contrato inteligente se forem detectadas condições que provavelmente afetarão negativamente o rendimento da colheita. Talvez outro cenário pudesse ser monitorar o clima usando dispositivos IoT, e, no caso de furacões, os reparos nas casas serem automaticamente iniciados e pagos por um contrato inteligente. Esse é o tipo que podemos chamar de substituição e/ou melhoria dos produtos de seguros tradicionais usando blockchain.

No entanto, existe outro ramo de produtos de seguro que busca mitigar os riscos associados às atividades DeFi. Por exemplo, proteção contra riscos representados por DApps com mau funcionamento, bugs em contratos inteligentes, ataques a exchanges ou quedas no preço de moedas. Se uma quantia significativa for mantida por um usuário em uma exchange de criptomoedas, pode ser benéfico cobrir os ativos contra o risco de hacks em exchanges de criptomoedas ou até mesmo de falência.

Há certos benefícios no seguro DeFi, incluindo:

* aumento na velocidade de processamento e execução de sinistros,
* pagamento automatizado de sinistros,
* redução de reivindicações falsas,
* onboarding mais rápido de clientes,
* análise de risco automatizada e rápida usando contratos inteligentes para determinar e definir parâmetros de apólice de forma algorítmica.

Há muitos projetos DeFi que oferecem seguros descentralizados, incluindo, mas não se limitando a:

* [Opium Finance insurance](https://opium.finance)
* [Nexus Mutual](https://www.nexusmutual.io)

**Empréstimos descentralizados – empréstimo e tomada de empréstimo**

O empréstimo e o financiamento no DeFi são bastante semelhantes aos serviços de empréstimo que existem nas finanças tradicionais, exceto pelo fato de que são gerenciados e oferecidos por aplicações descentralizadas (DApps) executadas na blockchain.

O mecanismo de empréstimo consiste em cinco principais atores:

1. **Cofre (vault):** um contrato inteligente que encapsula a lógica para gerenciar funções de empréstimo e tomada de empréstimo, os atores envolvidos e os ativos financeiros (ou seja, tokens).
2. **Credor:** é a entidade que empresta os fundos depositando o principal no cofre com a esperança de resgatar o principal e ganhar juros como lucro.
3. **Tomador de empréstimo:** é a entidade que oferece colateral (depósito de segurança) e toma os ativos emprestados:

a. O **colateral** é um ativo cripto que um tomador deposita como garantia para assegurar a dívida. O colateral garante que o tomador pode pagar o empréstimo.

b. Existem dois métodos que existem nos protocolos DeFi para colateralização:

i. **Sobrecolateralização:** significa que o valor do colateral fornecido pelo tomador é maior do que o valor do empréstimo. Uma vez que o empréstimo é emitido, o tomador pode usar livremente o empréstimo devido à segurança proporcionada pela sobrecolateralização.

ii. **Subcolateralização:** significa que o valor do colateral oferecido é menor do que o valor do empréstimo. Uma vez que o empréstimo é emitido, o tomador ainda não é livre para usar os fundos como quiser, porque o risco é maior devido à subcolateralização; portanto, o contrato inteligente mantém o controle de todos os ativos e libera os fundos com cautela.

1. **Liquidante:** é a entidade que propõe a liquidação ao cofre caso o colateral do tomador caia abaixo de um determinado valor, e recebe um incentivo para fazê-lo. Lembre-se de que, nas finanças tradicionais, a liquidação ocorre quando uma entidade vende alguns de seus ativos por um valor reduzido para quitar uma dívida. Em empréstimos DeFi, liquidação significa a mesma coisa, onde indivíduos tomam emprestado de um protocolo de empréstimo DeFi e o garantem oferecendo criptoativos como colateral. A liquidação ocorre no protocolo de empréstimo DeFi quando o cofre (o contrato inteligente do protocolo de empréstimo) vende automaticamente o colateral depositado para quitar a dívida.

Liquidantes são incentivados a comprar o colateral com desconto e cobrir a dívida. Essencialmente, o liquidante paga a dívida e obtém o ativo colateralizado a um preço com desconto. Esse desconto é chamado de **spread de liquidação**. Os liquidantes também podem competir em um mecanismo de leilão facilitado por um contrato inteligente para vencer o lance de liquidação. Há também, às vezes, um limite imposto sobre a fração máxima do empréstimo que pode ser liquidada em uma única transação de liquidação. Esse limite é chamado de **fator de encerramento (close factor)**. Geralmente, esse valor é definido como 0,5, significando que os liquidantes podem quitar até metade do empréstimo de um tomador de uma só vez.

A segurança dos ativos depositados contra os ativos emprestados e seu valor subjacente é representada por uma métrica numérica chamada **fator de saúde (Health Factor)**.

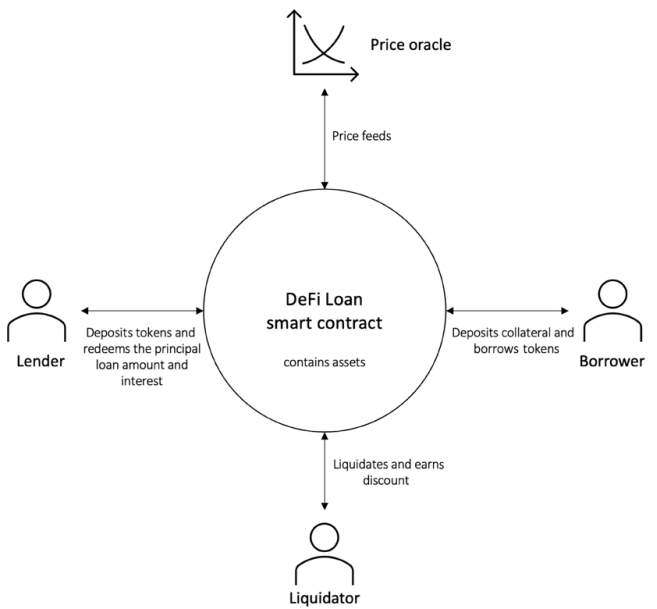
O **Fator de Saúde (HF)** é representado pela fórmula:  
**HF = (valor do colateral × limiar de liquidação) / valor total dos ativos emprestados**

Onde o **limiar de liquidação** é um valor entre 0 e 1 multiplicado pela soma do valor do colateral e dividido pelo valor total dos ativos emprestados. Essencialmente, o HF serve como um indicador da estabilidade dos fundos em relação ao risco potencial de liquidação. O HF aumenta ou diminui em relação às flutuações de valor dos ativos. Se ele aumenta, melhora a posição do tomador e torna a liquidação menos provável. Se o valor do colateral diminui, o HF também se reduz, aumentando o risco de liquidação. Na prática, se o valor de HF cair abaixo de 1, a posição de dívida torna-se passível de liquidação.

Se o valor do colateral cair tanto a ponto de pagar o valor principal se tornar mais caro, isso significa que o tomador entrou em **inadimplência**. A liquidação funciona como um mecanismo de segurança que é ativado segundo as regras definidas pelo contrato inteligente para vender o colateral depositado do tomador a fim de limitar as perdas enfrentadas pelo credor.

1. **Oráculo de preços:** é a entidade que fornece preços (dados de mercado) ao cofre para garantir que (entre outras coisas) o preço do colateral esteja atualizado, de modo que, se cair abaixo de um limite, a liquidação possa ser acionada, o que envolve o liquidante votando pela liquidação do tomador.

Podemos visualizar essa arquitetura de alto nível do mecanismo de empréstimo DeFi na Figura 21.7:



*Figure 21.7: DeFi and lending/borrowing*

Há muitos projetos DeFi que oferecem serviços de empréstimo e tomada de empréstimo, incluindo:

* [Aave](https://app.aave.com)
* [Euler](https://www.euler.finance)
* [Compound](https://compound.finance)

Há muitos outros, e uma pesquisa na internet pode revelar diversos resultados.

Tokens não fungíveis (**NFTs**) discutidos no **Capítulo 15, Tokenização**, possuem diversas aplicações no DeFi, onde aplicações DeFi aproveitam as propriedades dos NFTs para criar novos instrumentos e serviços financeiros. Algumas das aplicações mais comuns de NFTs no DeFi incluem:

* **Empréstimos colateralizados:** em plataformas de empréstimo DeFi, os usuários podem tomar empréstimos depositando colateral. No empréstimo tradicional, o colateral é tipicamente um ativo físico como imóveis ou ações. No DeFi, no entanto, os usuários podem usar NFTs como colateral para empréstimos. Isso permite que os usuários aproveitem seus ativos digitais para obter acesso a fundos sem precisar vendê-los.
* **Ativos tokenizados:** NFTs podem ser usados para representar ativos únicos e ilíquidos, como imóveis, obras de arte ou colecionáveis. Esses ativos podem ser tokenizados em NFTs, que podem então ser negociados em plataformas DeFi, proporcionando liquidez a ativos anteriormente ilíquidos.
* **Propriedade fracionada:** NFTs podem ser divididos em unidades menores, permitindo a **propriedade fracionada**. Isso significa que vários investidores podem possuir uma parte de um NFT, o que pode ser benéfico para ativos de alto valor como imóveis ou arte. A propriedade fracionada permite que investidores compartilhem o risco e o custo de aquisição e manutenção do ativo.
* **Yield farming:** *Yield farming* é uma prática DeFi onde usuários fornecem liquidez a um pool de fundos e recebem recompensas em troca. NFTs podem ser usados para incentivar a provisão de liquidez ao fornecer recompensas exclusivas aos usuários que fazem *staking* de NFTs específicos.
* **Gamificação:** NFTs também podem ser usados para **gamificar** aplicações DeFi, incentivando os usuários a participar e competir por recompensas. Por exemplo, usuários podem ganhar NFTs como recompensas por completar determinadas tarefas ou alcançar marcos específicos.

Esses são apenas alguns exemplos de como os NFTs estão sendo usados no DeFi. À medida que o espaço DeFi continua a crescer, podemos esperar ver aplicações novas e inovadoras dos NFTs em serviços financeiros.

Com todos esses serviços discutidos até agora, podemos ver que o DeFi oferece muitos benefícios. Resumimos eles a seguir:

**Benefícios do DeFi**

Os principais benefícios do DeFi incluem:

* **Redução de risco:** DeFi oferece liquidação atômica e transparência, o que resulta na redução do risco.
* **Menos centralizado ou totalmente descentralizado:** DeFi opera sem intermediários tradicionais (intermediários financeiros), o que resulta em serviços financeiros de baixo custo e sem atrito.
* **Aberto e inclusivo:** DeFi não possui as barreiras tradicionais que vemos nas finanças tradicionais, como exigências de capital, processos de integração complicados e exigências de identificação.
* **Transparente:** como todo o ecossistema é aberto, auditável e publicamente verificável, isso permite confiança entre os consumidores.
* **Interoperável:** o ecossistema DeFi não existe apenas em cadeias individuais como Ethereum e Solana, mas também é um ecossistema multiprotocolo com pontes entre cadeias, sistemas de camada 2 e sidechains. Essa propriedade agrega e melhora a liquidez entre redes. Além disso, em alguns casos, também há conectividade com a indústria de serviços financeiros tradicional, por exemplo, para obter dados de mercado e interoperar com infraestrutura financeira legada, o que gera um ecossistema ainda mais eficiente e rico.
* **Auto-custodial:** geralmente em plataformas DeFi, os próprios donos mantêm os ativos digitais, pois retêm suas chaves privadas.
* **Baixo custo:** DeFi permite movimentação e liquidação de valor sem intermediários, reduzindo os custos.
* **Programabilidade:** como o DeFi é fundamentalmente baseado em contratos inteligentes, permite automação e programabilidade de fluxos de trabalho.
* **Mais eficiente:** DeFi é mais eficiente, devido a execuções mais rápidas, flexibilidade e programabilidade.
* **Maior inclusão financeira:** qualquer pessoa com conexão à internet, um dispositivo móvel e hardware básico pode utilizar o sistema.
* **Resistência à censura:** DeFi é resistente à censura devido à tecnologia blockchain subjacente.

Claro que isso não significa que o CeFi será totalmente substituído pelo DeFi e que o CeFi deixará de existir por completo. O futuro das finanças ou do DeFi é coexistir com o CeFi, onde o sistema financeiro tradicional se conecta com o DeFi, e vice-versa. Por exemplo, um feed de dados de preços vindo de dados de mercado tradicionais para o protocolo DeFi por meio de oráculos. Stablecoins no mundo DeFi são baseadas/atreladas aos ativos e moedas fiduciárias do mundo financeiro tradicional. Reservas de stablecoins podem ser mantidas no mundo financeiro tradicional CeFi. Só o tempo dirá qual será o formato final da indústria de serviços financeiros em alguns anos; no entanto, um futuro colaborativo onde exista conectividade entre CeFi e DeFi é provável e já é o caso em muitos usos reais.

Como qualquer tecnologia, o DeFi também enfrenta seus próprios desafios, que se baseiam principalmente nas limitações da blockchain. Alguns desses desafios incluem regulação, interoperabilidade, escalabilidade e privacidade. Abordaremos esses desafios e as soluções relevantes em detalhes mais adiante neste livro.

**Na próxima seção, veremos como o DEX Uniswap funciona e usaremos um par de tokens para fornecer liquidez ao protocolo Uniswap.**

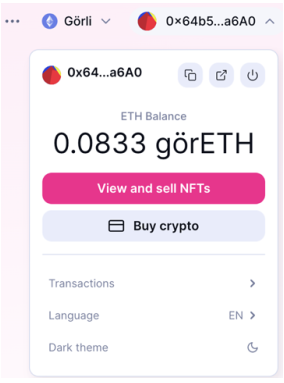
**Uniswap**

O **Uniswap** é um DEX que opera em cadeias compatíveis com EVM, principalmente na blockchain Ethereum. Ele permite que os usuários negociem criptomoedas sem depender de uma autoridade central ou intermediário. A plataforma usa um sistema AMM para determinar o preço dos ativos, o que permite negociações instantâneas sem a necessidade de um livro de ordens. Os usuários também podem fornecer liquidez ao Uniswap depositando seus ativos em pools de liquidez. Em troca por fornecer liquidez, os usuários recebem uma parte das taxas de negociação. O Uniswap é **não custodial**, o que significa que os usuários mantêm o controle de seus próprios fundos e não precisam confiar seus ativos a terceiros. A plataforma é **código aberto**, permitindo que qualquer pessoa contribua para seu desenvolvimento. O Uniswap também possui um sistema de governança descentralizado que permite aos detentores do token UNI votarem em propostas e mudanças na plataforma.

**Trocar o token**

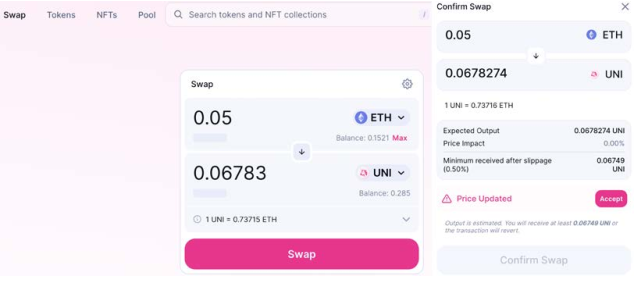
Siga os passos descritos abaixo para trocar o token:

1. Acesse o site do Uniswap (<https://app.uniswap.org/>) e conecte-se à rede de testes **Goerli** por meio do MetaMask. Uma vez conectado, você deverá ver os detalhes como na captura de tela abaixo:



*Figure 21.8: Uniswap connected to Goerli*

1. Clique em **Swap**, selecione os tokens e confirme a troca, como mostrado abaixo:

 O MetaMask será aberto, confirme a transação lá e aguarde o processamento (mineração). Ele também pedirá que você adicione o token à sua carteira MetaMask; clique em **Sim**, se desejar, e ele será adicionado como um ativo à MetaMask.

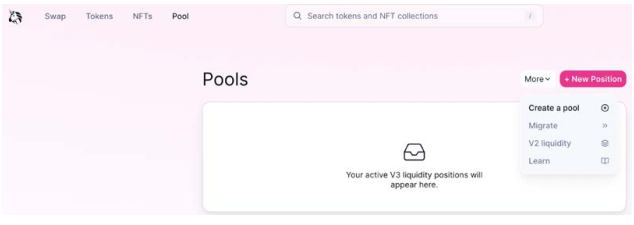
1. Agora, trocamos algum ETH por UNI.

**Vamos agora ver como criar um pool de liquidez.**

**Pool de liquidez Uniswap**

Siga os passos descritos abaixo para criar um novo pool de liquidez no Uniswap:

1. Clique em **Pool**, depois em **More**, e selecione a opção **Create a pool**:

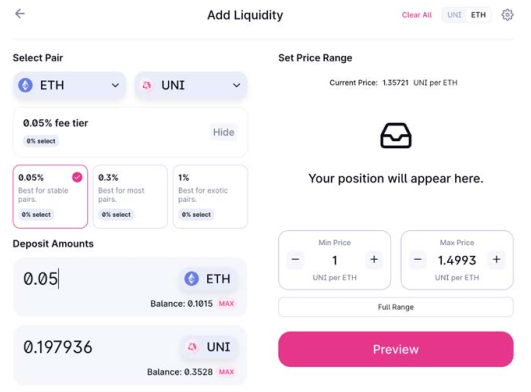


*Figure 21.10: Create a liquidity pool*

Isso abrirá a interface do usuário “Adicionar Liquidez”.

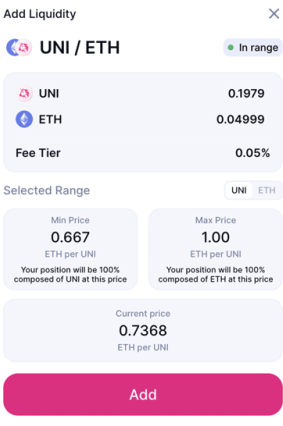
1. Sob a opção **Select Pair**, clique no menu suspenso e insira o endereço do contrato do token MET. Importe o token e ignore os avisos sugerindo que o token não está listado.
2. Insira os demais detalhes conforme mostrado abaixo na captura de tela:

a. **Select Pair**: ETH e UNI  
b. **Select fee tier**: 0.05  
c. **Insira a faixa de preço** entre o preço mínimo e máximo.



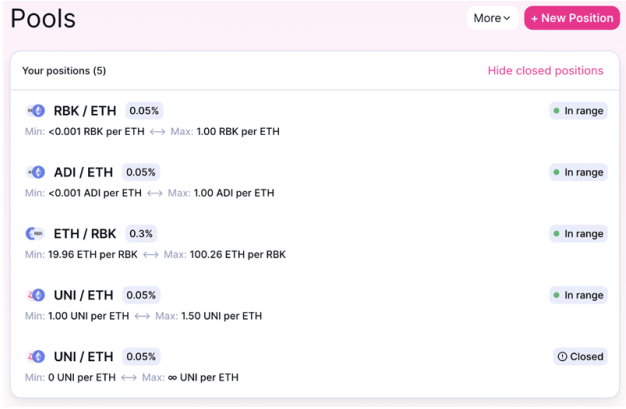
*Figure 21.11: Add liquidity parameter*

1. Clique no botão **Preview** e confirme no MetaMask.
2. Na janela pop-up **Add Liquidity** mostrada abaixo, clique em **Add**:



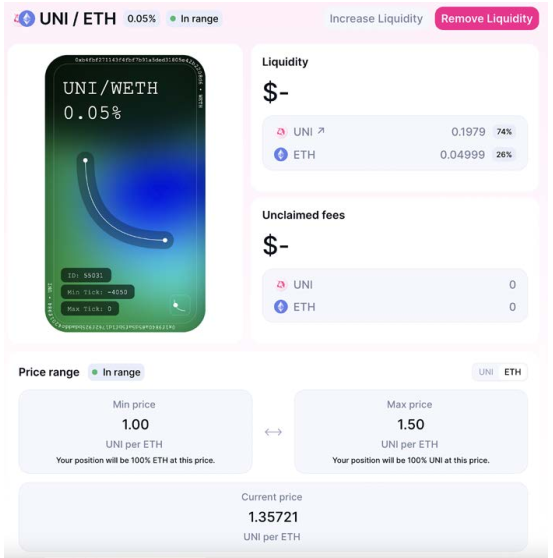
*Figure 21.12: Add Liquidity*

1. Confirme no MetaMask e aguarde a mineração.
2. Uma vez minerada, a liquidez será adicionada aos pools que você criou. Como mostrado abaixo, observe o par UNI/ETH na penúltima posição da lista:



*Figure 21.13: Liquidity pools*

1. Clique no pool para ver mais detalhes, como **Liquidity**, **Unclaimed fees** e **Price range**:



*Figure 21.14: Liquidity pool*

1. Você também pode adicionar mais liquidez, ou seja, tokens, clicando na opção **Increase Liquidity**.
2. Você também pode **remover liquidez** e **fechar sua posição**, além de reivindicar taxas, se houverem sido geradas, clicando em **Remove Liquidity**.

Neste exemplo, usamos tokens já disponíveis na plataforma Uniswap, trocamos ETH que tínhamos na rede Goerli por UNI e depois criamos um pool usando o par. No entanto, como a plataforma Uniswap é um DEX, qualquer token ERC-20 de qualquer usuário pode ser usado para criar um pool de liquidez.

**Finanças descentralizadas**

Como exercício, você consegue descobrir como fazer isso? Lembre-se de que criamos o token ERC-20 MET no Capítulo 15, Tokenização. Use aquele mesmo contrato de token ou crie um novo e implante na rede de testes Goerli. Já aprendemos a fazer isso no Capítulo 15. Melhor ainda, você pode usar a biblioteca **OpenZeppelin** para criar tokens ERC-20 de forma bem simples.

Siga o exemplo aqui:  
<https://docs.openzeppelin.com/contracts/4.x/erc20>  
Uma vez implantado, você pode explorar e confirmar a implantação do contrato no **Etherscan** também.

Uma vez que o contrato do token que você criou estiver implantado com sucesso, você pode, opcionalmente, importar o token no MetaMask. Após isso, você poderá criar seu próprio pool de liquidez com seu novo token ERC-20 na plataforma Uniswap seguindo os passos descritos anteriormente neste exemplo.

**Com isso, completamos nossa introdução ao DeFi.**

**Resumo**

Está claro que o DeFi está evoluindo rapidamente e continuará fazendo diferença em nossas vidas ao oferecer serviços financeiros que simplesmente não eram possíveis antes do advento do DeFi. Atualmente, estamos testemunhando a transformação histórica da internet da informação para a **internet de valor**, e, como tal, a blockchain e o DeFi continuarão tornando isso possível. Além disso, conceitos como DeFi institucional, novos tipos de tokens e protocolos e serviços DeFi inovadores tornarão os serviços financeiros mais acessíveis, inclusivos, extremamente eficientes e de baixo custo. Casos de uso para blockchains permissionadas privadas em finanças e blockchains públicas continuarão evoluindo e provavelmente irão convergir em algum momento no futuro para permitir casos de uso ainda mais inovadores e eficientes.