21

Decentralized Finance

Decentralized finance is a new financial system built using smart contracts and the blockchain technology that operates in a decentralized manner without relying on traditional financial intermediaries.

In this chapter, we'll cover the following topics:

- Introduction
- Financial markets and trading
- Application of blockchain in finance
- Decentralized finance
- DeFi primitives
- DeFi services
- DeFi benefits
- Using Uniswap

Now let's have a quick introduction to finance and financial markets. This will provide a foundation for the material presented next, such as DeFi, as many of the terms and ideas are the same, albeit in a different context.

Introduction

Finance is the study and management of money, investments, the creation of money, and other financial instruments to maximize wealth and minimize risk. The current global financial system operates through a complex network of financial markets, institutions, and intermediaries, with the goal of facilitating the efficient allocation of financial resources. Financial markets, such as stock exchanges and bond markets, serve as venues for buying and selling financial assets. Financial institutions, such as banks and investment firms, play a crucial role in intermediating between borrowers and lenders and providing financial services to their clients. Regulators, such as government agencies, are responsible for overseeing and regulating financial institutions and markets to ensure their safe and sound operation and to protect consumers. Investors, such as individuals, institutions, and organizations, invest in financial assets to generate returns and manage financial risk.

All these entities and components of the current global financial system work together to promote financial stability, growth, and prosperity and to serve the financial needs of individuals, businesses, and society.

The financial services industry offers a diverse range of financial assets and instruments to meet the needs of its clients. For example, stocks, bonds, mutual funds, and **Exchange-Traded Funds** (**ETFs**); money market instruments, such as certificates of deposit; and derivatives, such as options and futures contracts. These are just a few of the many financial assets and instruments offered by the financial services industry.

A financial market is a platform where financial instruments are traded between buyers and sellers. In a financial market, the prices of financial assets are determined by supply and demand and reflect the expectations of market participants regarding future events and conditions.

The current financial system is centralized and, traditionally, all financial institutions hold custody of customer funds and assets. They also serve as intermediaries for transactions. This centralization means that customer accounts can be frozen, transaction censoring can happen, and institutions can charge unfairly for the services provided. All these financial institutions are very highly regulated and must adhere to strict compliance rules such as **Know Your Customer** (**KYC**), **Anti Money Laundering** (**AML**), and **Combating the Financing of Terrorism** (**CFT**). Such regulations provide confidence to investors and keep the financial system working efficiently; however, note that because all these systems are inherently centralized, 100% fairness, transparency, competitive fees, and reliability cannot be guaranteed. Moreover, the customer must share personal and financial details with these service providers and as a result, the institutions know the real identity and complete account and transaction history of the customer. This is OK and works reasonably well in the current financial system; however, this lack of privacy might not be acceptable to some customers. Moreover, the customer is totally oblivious to what is going on behind closed doors; there is limited transparency when it comes to transaction processing. Customers don't know how their data is handled or how transactions are performed; all of this is opaque and means that the system is not as transparent as it should be. Databases are opaque and siloed, and data sharing between institutions becomes a problem. Customers are mostly totally unaware of how their data and transactions are handled and processed. This means that customers must fully trust these centralized entities.

Note that it is not the case that the current financial system is totally broken and nothing works. The current financial system works quite well and indeed upholds the highest standards of quality, adherence to regulation, and compliance requirements, but it can be improved in terms of privacy, financial inclusion, transparency, trust, and efficiency.

In 2008, a breakthrough invention, known as Bitcoin, provided a platform that could provide solutions to these problems. Bitcoin (the first electronic cash system, which is fully peer-to-peer and needs no trusted third party to operate) introduced blockchain, which is the fundamental layer that can provide solutions to most, if not all, of these problems.

Now let's dig deeper and understand some of the traditional finance concepts. First, let's have a look at financial markets.

So far, we learned what finance is. Finance is the broader concept that includes the management of money and assets, while financial markets refers to the platforms, venues, or systems where financial activities such as trading are performed.

Financial markets

Financial markets enable the trading of financial securities such as bonds, equities, derivatives, and currencies. There are broadly three types of markets: money markets, credit markets, and capital markets:

- Money markets are short-term markets where money is lent to companies or banks for interbank lending. Foreign exchange, or forex, is another category of money markets where currencies are traded.

- Credit markets consist mostly of retail banks that borrow money from central banks and loan it to companies or households in the form of mortgages or loans.

  > Retail banks are commercial banks that offer financial products and services to individuals and businesses, whereas central banks oversee the monetary system and regulation of the financial system of a country.

- Capital markets facilitate the buying and selling of financial instruments, mainly stocks and bonds. There are many types of financial instruments, such as cash instruments, derivative instruments, loans, securities, and many more. Securitization is the process of creating new security by transforming illiquid assets into tradeable financial instruments. Capital markets can be divided into two types: primary and secondary markets. Stocks are issued directly by the companies to investors in primary markets, whereas in secondary markets, investors resell their securities to other investors via stock exchanges. Various electronic trading systems are used by exchanges today to facilitate the trading of financial instruments.

A major activity performed in financial markets is trading, which we discuss next.

Trading

A market is a place where parties engage in exchange. It can be either a physical location or an electronic or virtual location. Various financial instruments, including equities, stocks, foreign exchanges, commodities, and various types of derivatives are traded at these marketplaces.

Derivatives are financial contracts whose value is derived from an underlying asset, such as stocks, bonds, commodities, currencies, or indices. They are used to hedge risk, speculate, and manage exposure to price movements of the underlying asset. Several classes of derivatives include futures, options, swaps, and forwards. They are traded in financial markets on organized exchanges, **Over-the-Counter** (**OTC**) markets, and various electronic trading platforms. Almost all financial institutions have introduced electronic trading software platforms to trade various types of instruments from different asset classes.

Trading can be defined as an activity in which traders buy or sell various financial instruments to generate profit and hedge risk. Investors, borrowers, hedgers, asset exchangers, and gamblers are a few types of traders. Traders have a short position when they owe something; in other words, if they have sold a contract, they have a short position. When traders buy a contract, they have a long position. There are various ways to transact trades, such as through brokers or directly on an exchange or **OTC** where buyers and sellers trade directly with each other instead of using an exchange. Brokers are agents who arrange trades for their customers and act on a client's behalf to deal at a given price or the best possible price.

Traders use exchanges to perform trading functions like buying and selling securities, which we introduce next.

Exchanges

An exchange is a centralized platform where securities, commodities, derivatives, and other financial instruments are bought and sold. Exchanges serve as intermediaries between buyers and sellers of financial assets, providing a standardized and regulated marketplace for trading. They ensure that transactions are executed fairly and transparently, provide market data, and facilitate the settlement of trades. Some well-known examples of exchanges include the **New York Stock Exchange** (**NYSE**), the Nasdaq Stock Market, the Tokyo Stock Exchange, the London Stock Exchange, and Euronext. Each exchange specializes in trading specific types of securities, such as stocks, bonds, futures, options, or currencies, and operates under its own set of rules and regulations.

Exchanges are usually considered to be very safe, regulated, and reliable places for trading. During the last few decades, electronic trading has gained popularity over traditional floor-based trading. Now, traders send orders to a central electronic order book from which the orders, prices, and related attributes are published to all associated systems using communications networks, thus, in essence, creating a virtual marketplace. Exchange trades can be performed only by members of the exchange. To trade without these limitations, the counterparties can participate in OTC trading directly.

Exchanges deal with orders; let's now explore what an order is and look at its various properties.

Orders and order properties

Orders are instructions to trade, and they are the main building blocks of a trading system. They have the following general attributes:

- The instrument's name
- The quantity to be traded
- Direction (buy or sell)
- The type of order that represents various conditions, for example, limit orders and stop orders

> In finance, a limit order is a type of order that allows the selling or buying of an asset at a specific price or better. A stop order is similar, but the key difference is that a limit order is visible to the market, whereas a stop order only becomes active (as a market order) when the specified stop price is met.

Orders are traded by bid prices and offer prices. Traders show their intention to buy or sell by attaching bid and offer prices to their orders. The price at which a trader will buy is known as the *bid price*. The price at which a trader is willing to sell is known as the *offer price*.

In order to facilitate the correct handling of orders, order management and routing systems are used, which we introduce next.

Order management and routing systems

Order routing systems route and deliver orders to various destinations depending on the business logic. Customers use them to send orders to their brokers, who then send these orders to dealers, clearing houses, and exchanges.

There are different types of orders. The two most common ones are *market orders* and *limit orders*. A market order is an instruction to trade at the best price currently available in the market. These orders get filled immediately at spot prices.

In finance, a *spot price* is the current price of an asset in a marketplace at which it can be bought or sold for immediate delivery.

On the other hand, a limit order is an instruction to trade at the best price available, but only if it is not lower than the limit price set by the trader. This can also be higher depending on the direction of the order: either to sell or buy. All of these orders are managed in an *order book*, which is a list of orders maintained by the exchange, and it records the intention of buying or selling by the traders.

A position is a commitment to sell or buy a number of financial instruments, including securities, currencies, and commodities for a given price. The contracts, securities, commodities, and currencies that traders buy or sell are commonly known as **trading instruments**, and they come under the broad umbrella of **asset classes**. The most common classes are real assets, financial assets, derivative contracts, and insurance contracts.

A trade is composed of several elements, which we discuss next.

Components of a trade

A trade ticket is the combination of all of the details related to a trade. However, there is some variation depending on the type of the instrument and the asset class. These elements are described here.

First, we have the underlying instrument that is the basis of the trade. It can be a currency, a bond, an interest rate, a commodity, or an equity.

The attributes of financial instruments include:

- **General attributes**: This includes the general identification information and essential features associated with every trade. Typical attributes include a unique ID, an instrument name, a type, a status, a trade date, and a time.
- **Economics**: Economics are features related to the value of the trade; for example, the buy or sell value, ticker, exchange, price, and quantity.
- **Sales**: Sales refers to the sales characteristic-related details, such as the name of the salesperson. It is just an informational field, usually without any impact on the trade lifecycle.
- **Counterparty**: The counterparty is an essential component of a trade as it shows the other side (the other party involved in the trade) of the trade, and it is required to settle the trade successfully. The normal attributes include the counterparty name, address, payment type, reference IDs, settlement date, and delivery type.

Trade lifecycle

A general trade lifecycle includes various stages from order placement to execution and settlement. This lifecycle is described step-by-step as follows:

- **Pre-execution**: An order is placed at this stage.
- **Execution and booking**: When the order is matched and executed, it is converted into a trade. At this stage, the contract between counterparties is matured.
- **Confirmation**: This is where both counterparties agree to the particulars of the trade.
- **Post-booking**: This stage is concerned with various scrutiny and verification processes required to ascertain the correctness of the trade.
- **Settlement**: This is the most vital part of the trade lifecycle. At this stage, the trade is final.
- **End-of-day processing**: End-of-day processes include report generation, profit and loss calculations, and various risk calculations.

This lifecycle is also shown in the following image:

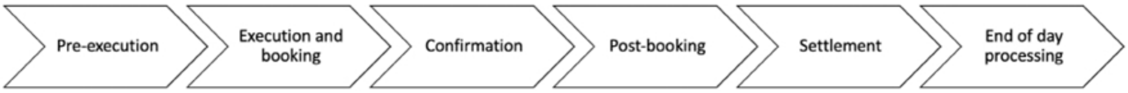

Figure 21.1: Trade lifecycle

In all the aforementioned processes, many people and business functions are involved. Most commonly, these are divided into functions such as front office, middle office, and back office.

While the trading industry is very secure and works well, there are some problems that can occur. One of them is order anticipation, where order anticipators try to make a profit before other traders can carry out trading. This is based on the anticipation of a trader who knows how the activities of other trades will affect prices. Frontrunners, sentiment-oriented technical traders, and squeezers are some examples of order anticipators.

Also, there is a possibility of market manipulation. It is strictly illegal in all countries. Fraudulent traders can spread false information in the market, which can then result in price movements, enabling illegal profiteering. Usually, manipulative market conduct is trade-based, and it includes generalized and time-specific manipulations. Actions that can create an artificial shortage of stock, an impression of false activity, and price manipulation to gain criminal benefits are included in this category.

Both of these concepts are relevant to financial crime. However, it is possible to develop blockchain-based systems that can thwart market abuse due to its inherent transparency and security properties.

It was quickly realized after the invention of Bitcoin that blockchain can enable many use cases in the financial services industry that can bring about efficiency, transparency, and security. We present some of these use cases next and explore what impact blockchain has on traditional finance and how it improves existing services. After this section, we'll dive into decentralized finance, also known as DeFi.

Applications of blockchain in finance

Blockchain has many potential applications in the finance industry. Blockchain in finance is currently the hottest topic in the industry, and major banks and financial organizations are researching to find ways to adopt blockchain technology, primarily due to its highly desired potential to save costs. These applications include but are not limited to payments, cross-border payments, remittance, trade finance, supply chain finance, security trading, clearing and settlement, accounting, identity, KYC and AML, insurance, post-trade settlements, financial crime prevention, lending, and borrowing. We discuss some of these next.

Insurance

In the insurance industry, blockchain technology can help to stop fraudulent claims, increase the speed of claim processing, and enable transparency. Imagine a shared ledger between all insurers that can provide a quick and efficient mechanism for handling intercompany claims. Also, with the convergence of IoT and blockchain, an ecosystem of smart devices can be imagined, where all these things can negotiate and manage their insurance policies, which are controlled by smart contracts on the blockchain.

Blockchain can reduce the overall cost and effort required to process claims. Claims can be automatically verified and paid via smart contracts and the associated identity of the insurance policyholder. For example, a smart contract, with the help of an **oracle** and possibly IoT, can make sure that when the accident occurred, it can record related telemetry data and, based on this information, release payment. It can also withhold payment if the smart contract, after evaluating conditions of payment, concludes that payment should not be released; for example, in a scenario where an authorized workshop did not repair the vehicle or was used outside a designated area, and so on and so forth. There can be many conditions that a smart contract can evaluate to process claims and the choice of these rules depends on the insurer, but the general idea is that smart contracts, in combination with IoT and oracles, can automate the entire vehicle insurance industry.

Post-trade settlement

This is the most sought-after application of blockchain technology. Currently, many financial institutions are exploring the possibility of using blockchain technology to simplify, automate, and speed up the costly and time-consuming post-trade settlement process.

To understand the problem better, the trade lifecycle will be described briefly. A trade lifecycle contains three steps: **execution**, **clearing**, and **settlement**. Execution is concerned with the commitment of trading between two parties and can be entered into the system via front-office order management terminals or exchanges. Clearing is the next step, whereby the trade is matched between the seller and buyer based on certain attributes, such as price and quantity.

At this stage, accounts that are involved in payment are also identified. Finally, the settlement is where, eventually, security is exchanged for payment between the buyer and seller.

In the traditional trade lifecycle model, a central clearing house is required to facilitate trading between parties, which bears the credit risk of both parties. The current scheme is somewhat complicated, whereby a seller and buyer have to take a complicated route to trade with each other. This comprises various firms, brokers, clearing houses, and custodians, but with blockchain, a single distributed ledger with appropriate smart contracts can simplify this whole process and can enable buyers and sellers to talk directly to each other.

Notably, the post-trade settlement process usually takes two to three days and has a dependency on central clearing houses and reconciliation systems. With the shared ledger approach, all participants on the blockchain can immediately see a single version of truth regarding the state of the trade. Moreover, P2P settlement is possible, which results in the reduction of complexity, cost, risk, and the time it takes to settle the trade. Finally, intermediaries can be eliminated by making use of the appropriate smart contracts on the blockchain. Also, regulators can view the blockchain for auditing and regulatory requirements.

> This can be very useful in implementing MIFID-II regulation requirements (`https://www.fca.org.uk/markets/mifid-`

`ii`).

Financial crime prevention

KYC and AML are the key enablers for the prevention of financial crime. In the case of KYC, currently, each institution maintains its own copy of customer data and performs verification via centralized data providers. This can be a time-consuming process and can result in delays in onboarding a new client.

Blockchain can provide a solution to this problem by securely sharing a distributed ledger between all financial institutions that contain verified and true identities of customers. This distributed ledger can only be updated by consensus between the participants, thus providing transparency and auditability. This can not only reduce costs but also enable regulatory and compliance requirements to be satisfied in a better and more consistent manner.

In the case of AML, due to the immutable, shared, and transparent nature of blockchain, regulators can easily be granted access to a private blockchain where they can fetch data for relevant regulatory reporting. This will also result in reducing complexity and costs related to the current regulatory reporting paradigm. This is where data is fetched from various legacy and disparate systems, and then aggregated and formatted together for reporting purposes. Blockchain can provide a single shared view of all financial transactions in the system that are cryptographically secure, authentic, and auditable, thus reducing the costs and complexity associated with the currently employed regulatory reporting methods. A simple solution is shown in *Figure 21.2*:

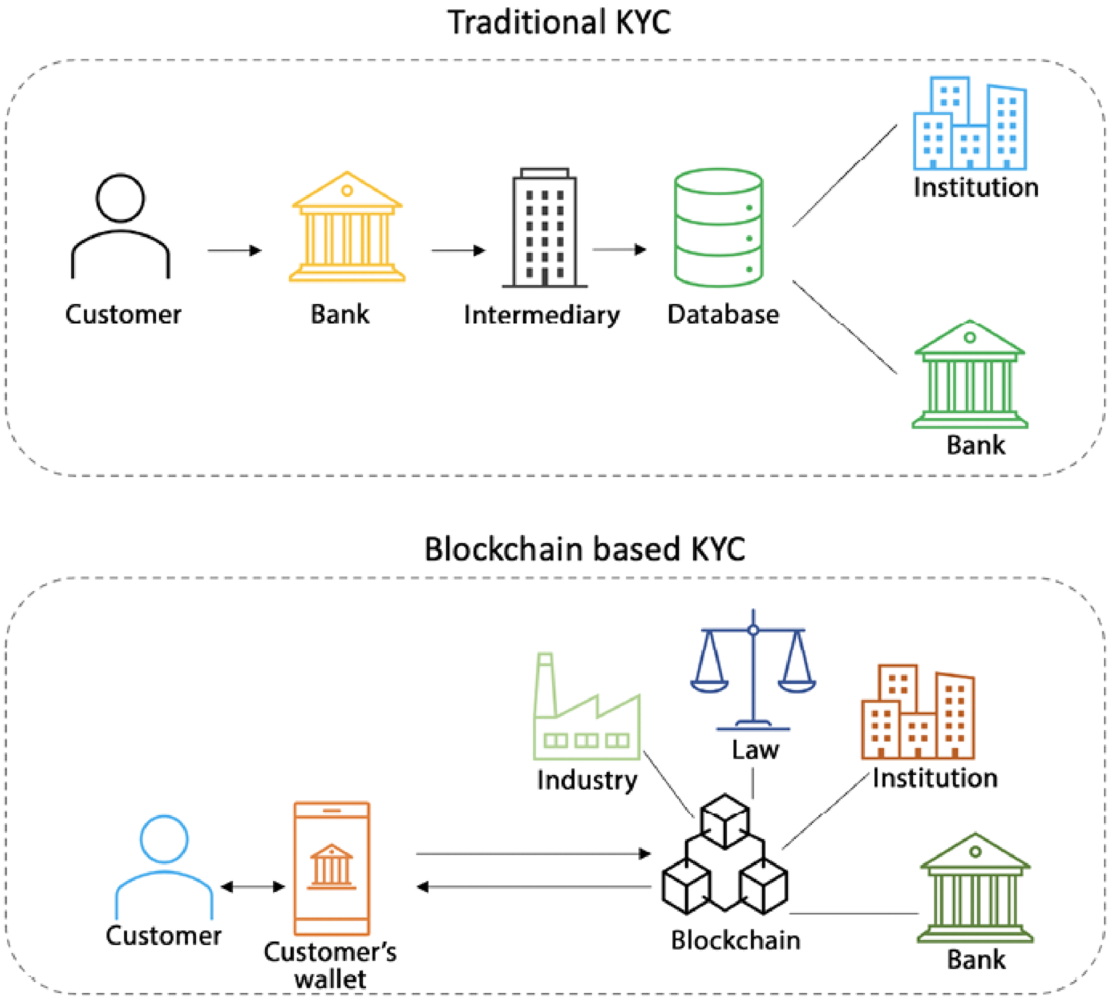

Figure 21.2: Traditional vs blockchain-based KYC

Blockchain-based KYC is much more efficient than traditional KYC. In a traditional system, a customer submits KYC documents/data to a bank. The bank verifies and stores the data and also sends it to a third-party centralized intermediary for storage. Other banks perform the same process and/or request data from the centralized intermediary, which is not efficient. Mostly, current KYC processes are siloed, and banks perform this process individually. Usually, all institutions run their own databases with not much sharing. There is also a centralized registry in some cases, but as it's centralized, it doesn't have the benefits that come with decentralization. As a result of this complex state of affairs, client onboarding takes a long time – it can even be two months in some cases. Also, it results in duplication of effort as each bank has to do its own KYC. In blockchain-based KYC, a customer submits KYC data to the blockchain. An institution verifies KYC data and posts the KYC status on the blockchain for that customer. The customer receives the KYC-compliant status (in the form of a verifiable credential or some other means).

Banks and other institutions access KYC data from the chain without needing to request it from other institutions and the customer can present the issued VC to any other institution as proof that the customer is properly KYC-cleared already and doesn't need KYC done again. This means that other banks can reuse KYC data, without duplication, and can even use verifiable credentials to verify (without even looking at the customer's data) that the customer is already KYC cleared and can access financial services. This is all made possible by blockchain.

Payments

A payment is a transfer of money or its equivalent from one party (the payer) to another (the payee) in exchange for services, goods, or for fulfilling a contract. Payments are usually made in the form of cash, bank transfers, credit card payments, and cheques. There are various electronic payment systems in use, such as **Bankers' Automated Clearing System** (**BACS**) and the **Clearing House Automated Payment System** (**CHAPS**). All these systems are, however, centralized and governed by traditional financial service industry codes and practices. These systems work adequately, but with the advent of blockchain, the potential of technology has arisen to address some of the limitations that exist in currently used systems.

The key advantages that blockchain technology can bring to payments are decentralization, faster settlement times, better resilience, and high availability. With all these advantages, it is easy to see how the payments industry can benefit from blockchain technology. There is also another branch of payments that deals with international or cross-border payments and comes with its own challenges. In traditional finance, cross-border payment is a complex process that can take days to process and involves multiple intermediaries. Current mechanisms suffer from delays incurred by multiple intermediaries, enforcement of regulations, differences in terms of regulations between different jurisdictions…the list goes on. All of these issues can be addressed by utilizing blockchain technology. The most significant advantage is decentralization, where, due to the lack of the requirement of intermediaries, payments can be made directly between businesses or individuals. Also, due to P2P connectivity, the whole process becomes a lot faster—almost immediate, in fact—which results in more productivity and business agility. We can see, in *Figure 21.3*, how a complex system can be transformed into a simpler system using blockchain.

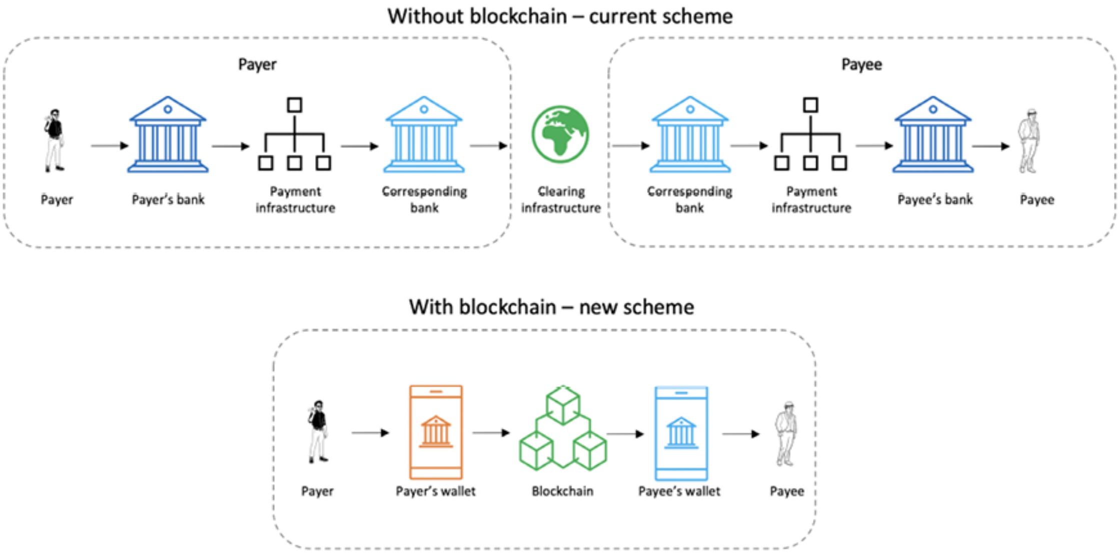

Figure 21.3: Cross-border payment system – from complex to simple using blockchain

The use of blockchain in the cross-border payment system removes settlement risks. The payee receives funds in seconds/minutes instead of days, even for international payments. Moreover, it's low cost as there are no intermediary banks that can charge fees. There is also no need for reconciliation as all data is there on the chain, already verified, and all participants can see and use it. There are no cutoff times or delays due to holidays etc. as the system is running 24/7 as long as the blockchain is running. It also enables **Peer-to-Peer** (**P2P**) payments, where payers and payees can deal with each other directly through wallets connecting to the blockchain, without any intermediaries at all. In some cases, due to regulatory requirements, institutions might be needed, but still, the overall experience for a customer is much easier, quicker, and seamless.

More and more use cases are emerging: clearing and settlements, identity, primary and secondary markets, trade finance, supply chain, and many others. It is now clear that blockchain indeed enables use cases that were not possible before.

While most of the innovations discussed so far are largely based on permissioned chains and aim to improve existing financial processes by implementing them on blockchains, another phenomenon called decentralized finance on public chains has emerged.

Let's now explore what DeFi is.

Decentralized finance

We can define **DeFi** as a financial mechanism built using smart contracts on public blockchains aiming to provide traditional and novel financial services in a decentralized, trustless, interoperable, and permissionless manner.

While **Traditional Finance** (**TradFi**) – or **Centralized Finance** (**CeFi**) – has strived for decades to achieve efficiency and improve its services and has achieved quite a lot, DeFi however, due to the advantages of blockchain, could result in a total transformation of financial services in the future and has enabled (and is enabling and will enable) use cases that were never possible before the invention of blockchain. It is an ecosystem that has emerged as a result of the development of many different types of financial applications built on top of blockchains. With blockchains being decentralized and the applications being related to finance, the term decentralized finance emerged, or DeFi for short.

DeFi can be defined as an umbrella term used to describe a financial services ecosystem that is built on top of blockchains. **Centralized Finance** (**CeFi**), is a term now used to refer to the traditional financial services industry, which is centralized in nature, while DeFi is a movement to decentralize the traditional centralized financial services industry.

Tokenization plays a vital role in the DeFi ecosystem. DeFi is based on asset tokenization. We discussed tokenization in detail in *Chapter 15*, *Tokenization*. DeFi is a vast subject with many different applications, protocols, assets, tokens, blockchains, and smart contracts.

The DeFi ecosystem is the fastest-growing infrastructure running on different blockchains. Originally, most DeFi applications ran on Ethereum, but with the advent of new chains like Solana, Cosmos, Polkadot, Avalanche, EOS, Hedera, and many others, we see an exponential expansion of the DeFi ecosystem. However, Ethereum remains the most preferred. DeFi is enabling use cases that are novel and were simply not possible before.

The range of DeFi DApps includes, but is not limited to, lending and borrowing, trading, asset management, insurance, tokenization, and prediction markets. All these decentralized applications, along with their smart contracts and infrastructure, make up the DeFi ecosystem.

In order to determine if an application or protocol is truly a DeFi protocol, we can ask three questions:

1. Is the user in full control of the financial asset?
2. Can a single entity censor transactions?
3. Can a single entity censor the protocol execution?

If the answer to all these questions is no, then the DApp is indeed a true DeFi DApp. If the answer to any of the questions is yes, then it’s not a true DeFi application or protocol.

Let’s now compare centralized finance with decentralized finance, which helps to understand how DeFi differs from CeFi.

	CeFi	**DeFi**
Admission	Permissioned	Permissionless
Base layer	Centralized databases	Decentralized blockchains

Authorization	Required	Usually not required
Asset holding	Custodial – trusted third party	Non-custodial – trustless, no single party in charge
Trust	Centralized	Decentralized
Governance	Centralized – under the control of a single party	Decentralized – no single party in control
Privacy	Limited, real identity must be revealed through KYC/AML processes	Mostly pseudonymous, or anonymous; however, regulatory pressure has introduced KYC/AML even in this space, but with advances in zero-knowledge technologies, true privacy with reasonable regulatory compliance is expected to be achieved.
Transparency	Opaque	Transparent/open
Risk	Less risky (due to stable and established platforms, control, and regulatory requirements)	More risky (due to lack of regulation and nascent technology)
Accessibility	Restricted due to regulation, controls, policies, etc.	Open to anyone with the internet

Properties of DeFi

DeFi should demonstrate five key properties, including:

- **Non-custodial**: users have full control over their assets.
- **Permissionless**: the system is fully inclusive, and anyone can access financial services.
- **Decentralized**: there is no single authority in control of the platform, protocol, or transaction execution. In other words, there are no trusted third-party requirements.
- **Transparent**: the system is open to audit and inspection by anyone to ensure its integrity.
- **Composable**: the system allows the creation of new financial products from a few basic building blocks.

DeFi layers

The DeFi ecosystem can be described in terms of a layered architecture, where each layer represents a class of operations and technology.

Let’s look at all these layers one by one:

1. **Settlement layer**: This is the base layer where blockchain platforms like Ethereum, Solana, and Polkadot exist.
2. **Asset layer**: This layer is composed of tokens and cryptocurrencies, native tokens, stablecoins, NFTs, and other tokens – for example, ERC20 and ERC721.
3. **Protocol layer**: This layer consists of DeFi protocols including exchanges, loan platforms, DeFi insurance platforms, and many other protocols. This is implemented using smart contracts. More specifically, **Decentralized Autonomous Organizations** (**DAOs**) exist at this layer.
4. **Application layer**: This layer is composed of decentralized applications that run on top of the protocols in the protocol layer and include applications and interfaces.
5. **Interoperability layer**: This layer is responsible for providing cross-chain interoperability, which includes bridges, hubs, relay chains, and various cross-chain messaging protocols.

6. **Aggregation layer**: This layer introduces the ability to aggregate multiple applications into an easy-to-use single platform for end users.

We can visualize this layered architecture with different actors and entities in *Figure 21.4* below:

Figure 21.4: DeFi layered architecture

Each layer in the DeFi ecosystem plays a crucial role in enabling the creation and growth of decentralized financial applications and services. The DeFi ecosystem has the potential to provide greater financial access and inclusion, as well as new financial opportunities and innovations. However, it is important to note that DeFi is rapidly evolving, and there are some risks and uncertainties associated with participating in the DeFi ecosystem. We'll cover these risks later in this book, where we discuss blockchain security and other challenges.

DeFi primitives

The DeFi ecosystem comprises many protocols, services, actors, and entities. These elements are listed below:

- **Transactions and smart contracts**: Transactions and smart contracts are the basic building block on which DeFi runs. Transactions and smart contract functionality are provided by the underlying blockchain, such as Ethereum.
- **Keepers**: Keepers can be defined as a class of **External Owned Accounts (EOAs)** that have the incentive to perform an action in a DeFi protocol. A keeper can also be an autonomous agent or a bot that monitors and triggers certain actions based on specific conditions within a smart contract and earns rewards to do so. Keepers act as the "maintenance crew" of the DeFi ecosystem by continuously monitoring the state of smart contracts and executing pre-defined transactions or activities when certain conditions are met. For example, a keeper may monitor a lending protocol and automatically repay a loan on be-

half of the borrower if it falls below a certain collateralization ratio. Keepers can help maintain the health and stability of DeFi protocols and are usually incentivized with rewards for their services.

- **Token**: A token is a digital representation of an asset, such as a cryptocurrency, a commodity, a stock, or a fiat currency. These tokens are created and managed on a blockchain and are used as a means of exchange, store of value, governance, or for other functions within DeFi protocols. Tokens can be used in a variety of DeFi protocols such as decentralized exchanges and lending platforms. They can also be used to incentivize users to participate in these protocols or as a right to vote on governance decisions within the protocol. Some of the popular tokens used in DeFi protocols include stablecoins like USDC, DAI, and USDT, and governance tokens like UNI, AAVE, and DOT. For more details on tokenization, refer to *Chapter 15*, *Tokenization*, which covered this subject in detail.
- **Oracle**: An oracle can be defined as a mechanism that feeds external information from the outside world into the blockchain. It plays a vital role in the DeFi ecosystem. For example, it enables the creation of applications that require real-time data, such as decentralized exchanges, lending platforms, and insurance protocols.
- **Governance**: Governance refers to the decision-making process for managing and evolving a decentralized protocol. It is typically achieved through consensus among stakeholders, such as token holders, who express their preferences through voting mechanisms. **DAOs** are a common mechanism used in DeFi protocols for governance. Governance can include decisions about technical changes, economic incentives, and the addition or removal of features and functionalities in the protocol. Decentralized governance enables the creation of more open, transparent, and democratic DeFi protocols controlled by users rather than centralized intermediaries or trusted third parties.
- **Custody**: Custody is a fundamental primitive in DeFi that allows users to escrow or keep funds in a smart contract. Such custody allows the creation of different solutions, especially lending protocols, insurance funds, market making, and automated disbursement of incentives.
- **Incentive**: Incentives in the DeFi ecosystem play an important role in keeping the DeFi ecosystem profitable for users. A common type is stake incentives, where a user stakes some assets to secure or partici-

pate in the governance of a DeFi protocol and earn rewards as a return. It is worth noting that incentives can be reduced or increased in a protocol based on the behavior of the user, market conditions, and protocol rules. Incentives can be negative or positive – for example, a staking reward is a positive incentive earned by contributing assets in a protocol to secure it. Negative incentives can occur due to slashing rules coded in a protocol and are used to discourage undesirable behavior of the stakers.

- **Bridge**: A bridge is a mechanism that connects two separate blockchain networks, allowing assets and data to be transferred between them. Bridges are important for enabling interoperability between different DeFi ecosystems, as they allow users to move assets and data between different networks. Bridges can be implemented as cross-chain atomic swaps, token wrapping, or by using bridge protocols that use a set of smart contracts to facilitate the transfer or exchange of assets between blockchain networks. Some common bridges are the Ethereum-Binance Smart Chain bridge, the Ethereum-Polygon bridge, and the Ethereum-Polkadot bridge. Bridges are important for expanding the functionality and reach of DeFi, as they enable assets and liquidity to be moved between different blockchain networks, making it easier for users to access a wider range of DeFi applications and services.

Let’s now discuss what services make up the DeFi ecosystem.

DeFi services

DeFi is composed of many different protocols, components, and services. We discuss these services next.

Asset tokenization

This is the foundation on which DeFi is built. It is the process of adding new assets to a blockchain platform. We can think of a token as a digital representation of a real-world asset. Tokenization makes assets more accessible, programmable, flexible, and easy to transfer. There are many types of tokens, including security tokens, governance tokens, NFTs, stablecoins, and quite a few others. For more details on tokenization, refer to *Chapter 15*, *Tokenization*, where these concepts are explained in detail.

> Tokenization can make illiquid assets liquid, which is not possible to do by traditional means. e.g., tokenize a piece of famous art.

Decentralized exchanges

We can divide exchanges into two types: centralized exchanges and decentralized exchanges.

An exchange is traditionally centralized, which means that some of them might not be entirely trustworthy. They are not transparent, and custody is also centralized. We have seen how centralized cryptocurrency exchanges have been subject to hacking and malpractices and, as a result, billions of funds are lost. For example, Mt. Gox, Coincheck, and Binance suffered losses due to successful hacking attacks in the past.

Decentralized Exchange (**DEX**) alleviates the problems that a **Centralized Exchange** (**CEX**) faces. We can define a DEX as a type of cryptocurrency (token) exchange that operates on a blockchain. DEXs allow for the direct exchange of cryptocurrencies between users (peers), without the need for a central authority or intermediaries. This is in contrast with centralized exchanges, which act as intermediaries and act as custodians of assets of their users.

In DeFi and blockchain-based trading systems in general, the trading of tokens is the prime activity. Tokens can be traded on exchanges. With the advent of DeFi, decentralized exchanges have emerged. DEXs are decentralized and therefore require no central authority or intermediary to facilitate trading. DEXs are decentralized, transparent, and non-custodial.

While the entry barrier to DEXs is low due to a lack of traditional regulatory requirements such as KYC requirements, this also makes them risky for investors because if somehow the DEX is hacked, then there is no protection against loss of funds. KYC is a standard due diligence practice in the financial services industry that ensures that the customer is legitimate and genuine. However, some centralized crypto exchanges have now started to do KYC and AML checks.

Some examples of DEXs are Uniswap, Bancor, WavesDEX, 0x, and IDEX. This ecosystem is growing at a very fast pace and is only expected to grow further.

The basic structure of a DEX is composed of a smart contract that facilitates trade between two parties. This smart contract consists of three functions: price discovery, trade matching, and trade clearing. We can visualize this in *Figure 21.5* below:

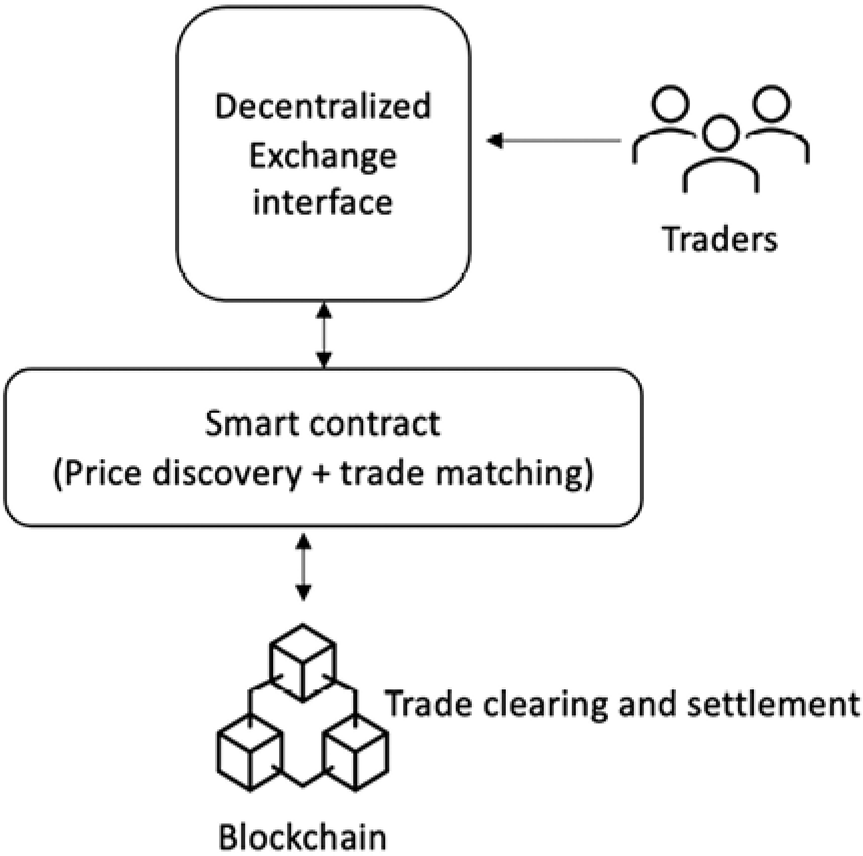
Decentralized Exchange interface
Traders
Smart contract
(Price discovery + trade matching)
Trade clearing and settlement
Blockchain

Figure 21.5: High-level architecture of a DEX

Price discovery is the process of determining the fair market value of a financial asset through the forces of supply and demand in the marketplace. It helps to establish the price at which a buyer and a seller are willing to trade the asset and ensures that assets are priced fairly and accurately. Price discovery occurs through various mechanisms, such as trading on exchanges, OTC transactions, and the use of derivatives, and is influenced by economic data, geopolitical events, and market sentiment. It is essential for the efficient allocation of capital and risk in financial markets.

There are several types of DEXs including AMM (also called liquidity pool-based DEX), order book-based DEX, and DEX aggregator. Classification is shown below:

1. Automated Market Maker:
    1. Order book DEX
    2. On-chain order book
2. Off-chain order book
3. DEX aggregators

Automated Market Maker (AMM) is a type of DEX where a liquidity pool provides a basis for automated market making. In a liquidity pool, the market-making is automated using a smart contract. A user with tokens (assets) adds liquidity to the liquidity pool, which can consist of several assets.

Any trader using the liquidity pool for swapping assets pays a fee to the user, who provided liquidity by adding their tokens into the liquidity pool. The core idea behind AMM is to let smart contracts do market-making instead of users placing orders manually. In short, liquidity pools can be thought of as shared pots of funds used by DEXs and deposited by users of the DEX, known as liquidity providers. Liquidity pools are used by DEXs to buy, sell, and fulfill orders. Liquidity providers earn pool fees in return for locking funds in the pool through a process called liquidity mining.

There are various AMM models. AMMs use math formulae to adjust prices in the liquidity pool. This math formula is programmed in the smart contract. There are several constant function market maker models including CPMM, CSMM, and CMMM.

CPMM

The constant product market maker formula is simply a product of two assets, as shown in the equation below:

$$x \times y = k$$

Where *x* represents the quantity of some asset *x*, *y* represents the quantity of some asset *y*, and *k* is a constant. The idea is that the product *k* of assets *x* and *y* must remain constant according to a defined constant. If a greater quantity of assets is added to the liquidity pool, then the constant will change; however, as long as they are traded, the net effect would keep *k* constant. In other words, the constant product formula ensures that the price of assets is adjusted according to supply and demand. For example, the purchase of asset *x* increases the price of *x* and decreases the price of *y*, and vice versa. The ratio of the number of assets of *x* and *y* sets the price accordingly. This constant product formula ensures that liquidity is always available. Functions like price discovery, trade matching, and market making are all served by this simple formula.

One of the key benefits of AMMs is that they provide instant liquidity instead of waiting for someone to place a qualifying/appropriate order to fulfill our trade exchange. In other words, it ensures liquidity even in the absence of other traders, by allowing buyers and sellers to exchange assets with the liquidity pool instead of each other. Another advantage of AMM is that it decreases the likelihood of price manipulation tactics, such as wash trading and front running, as the formula coded in the smart contract keeps the value of token pairs constant.

There is, however, the risk of slippage. Slippage can be defined as the difference between the current market price of an asset and the price at which the order is filled. However, if the liquidity pool has deep liquidity, and the trade sizes are also smaller, then slippage can be minimized; however, it is not 100% avoidable in CPMMs. The slippage can be expected or unexpected and needs to be managed accordingly.

Various DEXs use constant product formulas including SushiSwap, Bancor, and quite a few others.

CSMM

Constant sum market makers use a simple formula as shown below:

$x + y = k$

The formula simply means that the market maker would maintain a fixed sum of the two assets in the pool. While this is a simple function and provides protection against slippage, it doesn't provide unlimited liquidity.

CMMM

Constant mean market makers facilitate the formation of AMMs with more than two tokens and weightings that differ from the conventional 50/50 distribution. In this approach, the weighted geometric average of each reserve is unchanged. For instance, in a pool with three assets, *x*, *y*, and *z*, the formula would be:

This attribute permits variable exposure to different assets in the pool and allows swaps between any of the pool's tokens.

A comparison in visual form between different AMM models is shown in *Figure 21.6*, below:

Figure 21.6: CPMM vs CSMM vs CMMM

In the preceding diagram, *x*, *y*, and *z* are the asset quantities, with different mathematical relationships between them as per the formula.

Order book-based DEX

Order book-based DEXs use the traditional trading model, which was in existence for a long time before the emergence of DeFi. The order book model, usually known as **Central Limit Order Book** (**CLOB**), matches orders from buyers and sellers according to a set of predetermined rules. In order book-based DEXs, traders can set buy and sell orders for an asset, and the order book will organize them based on their prices. If there is supply and demand for an asset, it can be traded in these exchanges. Order book exchanges are suitable for markets with high liquidity since they can accurately determine market prices and handle large orders without significant slippage. They are preferred by institutional and retail traders alike due to their capital-efficient and transparent trade execution model. There are two types of order book-based DEXs: on-chain order book and off-chain order book.

DEX aggregator

While there are many DEX platforms, each has different levels of liquidity and prices. It could become difficult for users to figure out which DEX offers the best price and/or liquidity. This is where DEX aggregators can help. DEX aggregators, as the name suggests, are platforms where liquidity from different exchanges is aggregated. Instead of going to individual DEXs, users can use the aggregator to trade their assets. The job of an aggregator is to find the deepest liquidity, best prices, lowest fees, lowest slippage, and other most suitable attributes for the user according to their requirements.

There are two types of such aggregators commonly in use: off-chain aggregators and on-chain aggregators. Off-chain aggregators are usually implemented as websites providing the aggregation service. The key advantage of such an aggregator is that they are usually linked with many blockchains, are very flexible and efficient, and can find the optimal strategy for executing the trade for users. The downside, however, is that these aggregators are effectively trusted third parties, and these are centralized services, which can lead to transaction front running, suboptimal strategy selection, and even imposed biased strategy selection that might favor a particular exchange.

On-chain aggregators, as the name suggests, run on a chain, and provide aggregation services using a smart contract. This smart contract finds a provably optimal strategy for execution with the best routing, best profits, and arbitrage possibility. There is also an extremely low likelihood of front running or any biasedness due to all aggregation logic coded in the smart contracts running on a decentralized platform, i.e., on-chain. While this is an advantage, a key disadvantage is that these aggregators don't scale well and can usually cover roughly three exchanges.

Some limitations of DEX include lower liquidity, comparatively limited features to centralized exchanges, where features like limit orders, stop orders, etc. are available but such features are not available on DEXs, and very limited cross-chain interoperability, where most DEXs really operate just on one chain and seldom talk to other chains. However, the DEX ecosystem is thriving, and these limitations are not a great hindrance to the adoption and use of DEXs. Specifically, in AMM models, impermanent loss and low capital efficiency are two main limitations.

Impermanent loss occurs when the value of the assets you have deposited into a liquidity pool fluctuates, i.e., either increases or decreases compared to the value when you deposited them. This means that the value of the deposited assets could be different when they are withdrawn compared to when they were initially deposited into the pool. It's worth noting that the term "impermanent" can be misleading, as a decrease in the price of a token may only be temporary and could go up again due to market conditions or other factors. In this case, the loss would be considered temporary, or impermanent, because the price eventually went back up. However, if the dollar value (value generated after conversion of the crypto asset into USD) of the token at the time of withdrawal is less than the value when it was deposited, then the loss becomes permanent.

AMMs also need a large amount of liquidity to match the pricing impact of an order book-based exchange, which results in low capital efficiency.

To address these limitations, several innovations have been proposed, including dynamic automated market makers, hybrid constant function market makers, proactive market makers, and virtual automated market makers.

A DAMM model can use price feeds through oracles and implied volatility to distribute liquidity more effectively along the price curve. The model can create a more resilient market maker that can adapt to changes in market conditions by integrating various dynamic variables into the algorithm. When volatility is low, the model can focus liquidity near the market price to improve capital efficiency, which can be extended during periods of high volatility to protect traders from impermanant loss. In simple terms, the mathematical relationship (e.g.,) between assets is adjusted dynamically to ensure that the pool price continually and automatically aligns with the market price. This technique is intended to eliminate arbitrage opportunities.

Hybrid **Constant Function Market Makers** (**CFMMs**) combine several properties of AMMs, functions, and parameters to achieve a more stable, efficient, and profitable mechanism for traders.

Virtual AMMs aim to minimize price impact and mitigate impermenant loss. They use the same constant product formula as traditional AMMs – i.e., where . is some mathematical relationship – but instead of relying on a liquidity pool, traders deposit collateral to a smart contract. This allows trading synthetic assets instead of the underlying asset, which enables users to gain exposure to the price movement of many crypto assets efficiently.

The **Proactive Market Maker** (**PMM**) model has been developed to increase liquidity in protocols. This model mimics the behavior of a human market maker in a traditional central limit order book by using accurate market prices from an oracle. In response to market changes, the PMM protocol proactively moves the price curve of an asset, increasing the liquidity near the current market price. This facilitates efficient trading and reduces the impermanent loss for liquidity providers.

Another issue that AMMs suffer from is front running. This occurs when another user places a trade similar to a prospective buyer's but quickly sells it back, causing the price to rise, and then profiting from the price increase. This is possible because transactions in AMMs are public. Also known as a "sandwich attack," this is often automated using bots, which exacerbates the situation. In many cases, miners are the ones responsible for front running, and this has led to the term **Miner Extractable Value** (**MEV**), referring to the unfair profits that a third party can make from the original transaction.

Pros and cons of AMMs

One of the key advantages of AMMs is that there is no order book required to be maintained. The formulae related to CP are simply implementable in smart contracts. However, some disadvantages include the risk of impermanent loss, high slippage, and other technology security risks, which we'll cover in *Chapter 19*, *Blockchain Security*.

CEX vs DEX

A comparison of CEX and DEX is shown below and highlights the key differences between the two paradigms.

Attribute/exchange type	CEX	DEX
Asset custody	Third party	User
Entry barrier	High	Very low
Regulation	High	None, or very low
Infrastructure availability	High (but could be compromised due to centralization)	Very high (due to blockchain security guarantees)
User experience	Easy to use; supported	Could be difficult to use for new users; less support
Liquidity	Much deeper and professionally provided	Not very deep
Impermanent loss	Not applicable as highly liquid	Applicable and highly likely in case of fluctuations

Fees	Higher due to intermediaries	Much lower, as no intermediaries exist
Identity verification	Required	Not needed

As DeFi is a thriving ecosystem with massive profiting opportunities, a question arises: is it possible to automatically find the most profitable trading strategy and create DeFi trades accordingly to maximize profits? There are two methods employed to do so – the Bellman-Ford algorithm and SMT solvers.

Flash loans

A flash loan is a service that only exists in the DeFi world. In CeFi, a loan is an instrument that refers to an agreement between a lender and a borrower, in which the borrower receives a certain amount of funds (the loan) from the lender, with the obligation to repay the loan amount plus interest over a specified period. Loan instruments typically involve the payment of interest and principal on a regular basis and are secured or unsecured. Secured loans are backed by some type of collateral, such as a property or a vehicle, while unsecured loans are not backed by any collateral and are usually offered at a higher interest rate. The lender bears the risk of default and is compensated by the interest amount charged over the loan period. If the loan is for a long duration, then the interest rate is also higher because there is a greater exposure to risk for the lender that the borrower may default due to a longer time period. This means that if the lending is for a shorter period, then the risk is less and therefore requires less compensation for the lender.

A flash loan enables such short terms loans, which are instantaneous and are paid back in the same transaction. In other words, repayment of the loan occurs in the same transaction in which the lending occurred. Flash loans are atomic in nature due to the underlying blockchain, meaning that if the loan (principal) is not repaid with the required interest within the same transaction, the whole process rolls back to the previous state as if no money ever left the lender’s account. This means that there is no counterparty or duration risk in flash loans, which is totally different from loans in the traditional finance world.

This safety condition is enforced via blockchain-enabled atomic transactions. The operations within a transaction are executed completely in sequential order or fail altogether. A blockchain transaction can fail due to three reasons. Transaction fees are not sufficient, the transaction (function call) fails to meet the conditions in the smart contract, or the transaction is illicit (e.g., attempting to double spend). In all these cases, the state will be reverted automatically to the previous state as if no transaction was ever executed. This inherent safety mechanism enables flash loans.

If a user borrows a million dollars worth of tokens and fails to meet the loan conditions set forth in the smart contract (e.g., pay it back by the end of the transaction with interest), the transaction will be rolled back due to the inherent safety of the blockchain transaction execution mechanism. Imagine within a single transaction, the loan is issued from the liquidity pool, the loan is used, and the principal amount with interest is paid back to the liquidity pool. Imagine if the last condition is not met, i.e., the loan and interest are not paid back; the entire flash loan transaction fails and no state change occurs, as if no loan was ever issued. This safety guarantees the lender that the loan will always be paid back, otherwise, no loan will ever be issued. Secondly, there is no limit on the amount the borrower can request given that enough funds are available in the pool. This is very empowering, and no such construct exists (or can exist) in traditional finance.

Flash loans are uncollateralized, which means that they allow a user to take advantage of arbitrage opportunities (price difference) or to refinance without having to pledge any asset as collateral. Flash loans are accessible to anyone; all that’s required is a wallet and the required amount of funds, regardless of their credit-worthiness or financial status. This again is in stark contrast to loan instruments in traditional finance and allows anyone to access prospects that were not possible before in the CeFi world. Flash loans offer risk-free arbitrage. In short, there is no analog of flash loans that exists in traditional finance.

Some examples of flash loan providers include Equalizer (https://equalizer.finance) and Aave (https://aave.com).

Derivatives

Derivatives in the DeFi world serve the same purpose as derivatives in traditional finance, i.e., hedge price risk and interact with a specific asset without buying it. The value of DeFi derivatives is usually derived from cryptocurrency markets, but they can also be linked to other traditional assets like commodities and fiat currencies. Protocols for DeFi derivatives allow users to create synthetic assets that are tied to some underlying real-world assets. Some examples of DeFi derivative protocols are Synthetix (https://synthetix.io), Hegic (https://www.hegic.co), Opyn (https://www.opyn.co), and many others. These protocols enable investors to trade derivatives that are linked to various underlying assets such as commodities, cryptocurrencies, and indexes.

There are two types of decentralized derivatives: asset-based derivatives and event-based derivatives. Asset-based derivatives are offered by services like Synthetix and Mirror, whereas event-based derivatives are offered by services such as Augur.

Asset-based derivatives have their value tied to the value of an underlying asset, which can be a major cryptocurrency like Bitcoin, Ethereum, or any other financial asset. While the underlying asset in asset-backed derivatives is always financial, in the case of event-based derivatives, the underlying asset is some event, i.e., an observable variable. In these markets, individuals place bets on the outcome of events such as games and elections, among others.

Money streaming

Decentralized payments are already a norm in the DeFi world; however, what if we can make them even cheaper, faster, programmable, conditional, time-based, real-time, and more flexible?

The concept of streaming payments has emerged in DeFi, which means that instead of waiting for a traditional fixed period (e.g., weekly or monthly) for payment, the payers can “stream” payments in real time, in small increments, just like we stream videos online. Funds can be streamed in agreed-upon intervals between involved parties. One such platform is Sablier, which allows streaming tokens at regular intervals. One of the key advantages of streaming payments is that payees can verify that they are being paid now, instead of waiting and trusting the payer for a specific date and time to be paid in the future. Moreover, by earning a salary in real time, the concept of paydays is eliminated, which leads to a significant reduction in the need for payday loans. This method allows individuals to verify that they are being paid immediately and regularly at the time intervals that are suitable for them, rather than relying on the promise of future payment. Companies can also avoid wasting a considerable amount of money on accounting, invoicing, and timestamping because the money-streaming process can be more efficient and eliminate traditional accounting needs. Another idea could be stream billing, where the bills are paid in more frequent, shorter real-time intervals, which can alleviate the problem of paying the bills every month in one go. Similar terms such as real-time finance, token streaming, and social money have emerged in literature, which fundamentally mean the same thing – the ability to make payments in real time and flexibly.

Yield farming

Yield farming is a popular method for generating passive income from traders. These yield farming protocols are programmed using smart contracts. Smart contracts secure users’/traders’ tokens and offer interest on the locked assets. If these locked-in tokens (funds) are used to provide liquidity, traders can earn interest based on transaction fees. Liquidity is usually required for DEXs to facilitate trading. As these locked tokens can be used in DEXs to execute buy and sell orders, yield farmers can earn income through transaction fees. Moreover, if the locked tokens are used for loans, the investors can receive loan interest.

The interest paid to traders can balance out the potential risks of locking their tokens, such as *impermanent loss*, *token volatility* and the risk of *rug pulls*. The annual percentage rate can either be decided by the creator of the pool or automatically determined by the yield farming protocol, the logic of which is coded within the smart contracts that implement the protocol on the blockchain.

Insurance

We discussed some insurance use cases before in this chapter, in the context of blockchain use cases in finance. Those use cases are concerned with providing and improving insurance products that exist in the traditional financial world. For example, a use case where weather monitored by an IoT sensor on agricultural land automatically triggers an insurance payment through a smart contract if it detects conditions that are likely to adversely affect the yield of the crop. Perhaps another scenario could be to monitor the weather using IoT devices, and in case of hurricanes, house repairs are automatically triggered and paid off by the smart contract. So, this is the type that we can call the replacement and/or improvement of traditional insurance products using blockchain. However, there is another branch of insurance products that is looking to mitigate the risks associated with DeFi activity. For example, protection against risks posed by malfunctioning DApps, smart contract bugs, exchange hacks, or coin price crashes. If a significant amount is held by a user in a cryptocurrency exchange, it could be beneficial to cover the assets against the risk of cryptocurrency exchange hacks or even bankruptcy.

There are certain benefits of DeFi insurance, including increased speed of claim processing and action, automated payment of claims, reduction of false claims, quicker onboarding of customers, and automated quick risk analysis using smart contracts to algorithmically determine and set policy parameters.

There are many DeFi projects that offer decentralized insurance including but not limited to Opium Finance insurance (`https://opium.finance`) and Nexus Mutual (`https://www.nexusmutual.io`).

Decentralized lending – lending and borrowing

DeFi lending and borrowing are quite like the lending services that exist in traditional finance except that they are managed and offered by decentralized applications (DApps) running on the blockchain.

The loan mechanism consists of five main actors:

1. **A vault**: a smart contract that encapsulates the logic to manage lending and borrowing functions, relevant actors, and financial assets (i.e., tokens).
2. **Lender**: this is the entity that lends the funds by depositing the principal to the vault in the hope of redeeming the principal and earning interest as profit.
3. **Borrower**: this is the entity that offers collateral (security deposit) and borrows the assets:
    1. Collateral is a crypto asset that a borrower deposits as security to secure the debt. The collateral guarantees that the borrower can pay back the loan.
    2. There are two methods that exist in DeFi protocols for collateralization:
        1. Over-collateralization means that the value of the collateral provided by the borrower is more than the loan value. Once the loan is issued, the borrower can use the loan freely due to the security provided by the over-collateralization.
        2. Under-collateralization means that the value of the offered collateral is less than the loan value. Once the loan is issued, the borrower is still not free to use the funds as they please, because the risk is higher due to under-collateralization; therefore, the smart contract keeps control of all the assets and releases funds cautiously.
4. **Liquidator**: this is the entity that proposes liquidation to the vault in case the borrower's collateral falls below a certain value, and it earns an incentive to do so. Recall that in traditional finance, liquidation occurs when an entity sells off some of its assets at a reduced value to settle a debt. In DeFi loans, liquidation means the same thing, where individuals borrow from a DeFi lending protocol and secure it by offering crypto assets as collateral. The liquidation occurs in the DeFi loan protocol when the vault (lending protocol smart contract) automatically sells deposited collateral to pay off the debt. Liquidators are incentivized to buy the discounted collateral and cover the debt.

Essentially, the liquidator repays the debt and gets the collateralized asset at a discounted rate. This discount is called the *liquidation spread*. Liquidators can also compete in an auction mechanism facilitated by a smart contract to win the bid to liquidate. There is also a limit sometimes imposed on the maximum fraction of the loan that can be liquidated in a single liquidation transaction. This limit is called the *close factor*. Usually, this is set to 0.5, meaning that liquidators can pay off up to half of a borrower's loan in one go.

The safety of the deposited assets against the borrowed assets and their underlying value is represented by a numeric metric called the "health factor."

The **Health Factor** (**HF**) is represented by a simple formula:

Where the liquidation threshold is a value between 0 and 1 multiplied by the sum of the collateral value and divided by the total value of the assets borrowed. Essentially, the HF serves as an indicator of the stability of the funds in relation to the potential risk of liquidation. The HF increases or decreases in relation to value fluctuations of the assets. If it increases, it improves the borrow position and makes liquidation less likely. If the value of the collateral decreases, the HF also reduces, increasing the liquidation risk. In practice, if the HF value falls below 1, the debt position becomes likely to be liquidated.

If the collateral value declines so low that paying back the principal amount becomes more expensive, then it means that the borrower has defaulted. Liquidation serves as a security mechanism that triggers under the rules defined by the smart contract to sell the deposited collateral from the borrower to limit the losses faced by the lender.

5. **Price oracle**: this entity feeds prices (market data) into the vault to ensure that (among other things) the price of collateral is up to date so that if it falls below a threshold, the liquidation can be triggered, which involves the liquidator voting for liquidation of the borrower.

We can visualize this high-level architecture of the DeFi lending mechanism in *Figure 21.7*:

Figure 21.7: DeFi and lending/borrowing

There are many DeFi projects that offer lending and borrowing services including Aave (https://app.aave.com), Euler (https://www.euler.finance), and Compound (https://compound.finance). There are many others, and an internet search can reveal many results.

Non-Fungible Tokens (**NFTs**) discussed in *Chapter 15*, *Tokenization*, have several applications in DeFi, where DeFi applications leverage the properties of NFTs to create new financial instruments and services. Some of the most common applications of NFTs in DeFi include:

- **Collateralized loans**: In DeFi lending platforms, users can borrow funds by depositing collateral. In traditional lending, the collateral is typically a physical asset such as real estate or stocks. In DeFi, however, users can use NFTs as collateral for loans. This allows users to leverage their digital assets to access funds without selling them.
- **Tokenized assets**: NFTs can be used to represent unique and illiquid assets, such as real estate, artwork, or collectibles. These assets can be tokenized into NFTs, which can then be traded on DeFi platforms, providing liquidity to previously illiquid assets.
- **Fractional ownership**: NFTs can be divided into smaller units, allowing for fractional ownership. This means that several investors can own a portion of an NFT, which can be beneficial for high-value assets such as real estate or art. Fractional ownership allows investors to share the risk and cost of acquiring and maintaining the asset.
- **Yield farming**: Yield farming is a DeFi practice where users provide liquidity to a pool of funds and receive rewards in return. NFTs can be used to incentivize liquidity provision by providing exclusive rewards to users who stake specific NFTs.
- **Gamification**: NFTs can also be used to gamify DeFi applications, incentivizing users to participate and compete for rewards. For example, users can earn NFTs as rewards for completing certain tasks or achieving specific milestones.

These are just a few examples of how NFTs are being used in DeFi. As the DeFi space continues to grow, we can expect to see new and innovative applications of NFTs in financial services.

With all these services discussed so far, we can see that DeFi has many benefits. We summarize them below.

Benefits of DeFi

Key benefits of DeFi include:

- **Reduction in risk**: DeFi offers atomic settlement and transparency, which results in the reduction of risk.
- **Less centralized or fully decentralized**: DeFi operates without traditional intermediaries (middlemen), which results in low-cost and frictionless financial services.
- **Open and inclusive**: DeFi has no traditional barriers that we see in traditional finance with capital requirements, cumbersome onboarding, and identification requirements.
- **Transparent**: As the entire ecosystem is open and auditable and publicly verifiable, it enables trust among consumers.
- **Interoperable**: The DeFi ecosystem not only exists on individual chains such as Ethereum and Solana but also is a multiprotocol ecosystem with cross-chain bridges, layer 2 systems, and sidechains. This very property aggregates and improves liquidity across networks. Moreover, in some cases, there is also connectivity with the traditional financial services industry, e.g., to get market data and interoperate with existing legacy and traditional financial infrastructure, which gives rise to an even more efficient and rich ecosystem.
- **Self-custodial**: Usually in DeFi platforms, owners hold digital assets as they hold their private keys.
- **Low cost**: DeFi enables value movement and settlement without intermediaries, thus reducing costs.
- **Programmability**: As DeFi is fundamentally based on smart contracts, it allows automation and programmability of workflows.
- **More efficient**: DeFi is more efficient, due to faster executions, flexibility, and programmability.

- **Better financial inclusion**: Anyone with an internet connection, a mobile device, and entry-level hardware should be able to use the system.
- **Censorship resistance**: DeFi is censorship-resistant due to the underlying blockchain technology.

Of course, this doesn’t mean that CeFi is totally going to be replaced with DeFi and CeFi will cease to exist altogether. The future of finance or DeFi is to coexist with CeFi, where the traditional financial system connects with DeFi, and vice versa. For example, a pricing data feed coming from traditional market data to the DeFi protocol via oracles. Stablecoins in the DeFi world are based on/pegged to the traditional financial world’s assets and fiat currency. Reserves of stablecoins could be kept in the CeFi traditional financial world. Only time will tell what the eventual shape of the financial service industry will be in a few years; however, a collaborative future where connectivity between CeFi and DeFi exists is likely and is already the case in many use cases.

Like any technology, DeFi also suffers from its own challenges, which are mostly based on blockchain limitations. Some of the challenges include regulation, interoperability, scalability, and privacy. We’ll cover these challenges and relevant solutions in detail later in this book.

In the next section, we’ll see how the Uniswap DEX works and will use a token pair to provide liquidity to the Uniswap protocol.

Uniswap

Uniswap is a DEX that operates on EVM chains, mainly on the Ethereum blockchain. It allows users to trade cryptocurrencies without relying on a central authority or middleman. The platform uses an AMM system to determine the price of assets, which allows for instant trading without the need for an order book. Users can also provide liquidity to Uniswap by depositing their cryptocurrency holdings into liquidity pools. In exchange for providing liquidity, users receive a portion of the trading fees. Uniswap is non-custodial, meaning users are in control of their own funds and do not have to trust a third party with their assets. The platform is open source, allowing anyone to contribute to the development of the platform. Uniswap also has a decentralized governance system that allows UNI token holders to vote on proposals and changes to the platform.

Swap the token

Follow the steps described below to swap the token:

1. Browse to the Uniswap website (https://app.uniswap.org/) and connect to the Goerli test network through MetaMask. Once connected, you should be able to see the details shown in the screenshot below:

Figure 21.8: Uniswap connected to Goerli

2. Click on **Swap**, select tokens, and confirm the swap, as shown below:

Figure 21.9: Swap tokens

3. MetaMask will open, confirm the transaction there, and wait for it to be processed (mined). It will also ask you to add it to your MetaMask wallet; click **Yes** if you want to and it will be added as an asset to MetaMask.
4. Now we have swapped some ETH for UNI.

Let's now see how we can create a liquidity pool.

Uniswap liquidity pool

Follow the steps described below to create a new liquidity pool in Uniswap:

1. Click on **Pool**, then **More**, and select the option **Create a pool**:

Figure 21.10: Create a liquidity pool

2. It will open the **Add Liquidity** user interface.
3. Under the **Select Pair** option, click on the dropdown and enter the address of the MET token contract. Import the token, and ignore any warnings suggesting that the token is not listed.
4. Enter the rest of the details as shown below in the screenshot:
    1. Select **Pair**: **ETH** and **UNI**
    2. Select fee tier: **0.05**
    3. Enter the price range between the minimum price and maximum price.

Figure 21.11: Add liquidity parameter

5. Click on the **Preview** button and confirm in MetaMask.
6. In the **Add Liquidity** popup shown below, click **Add**:

Figure 21.12: Add Liquidity

7. Confirm in MetaMask, and wait for it to be mined.
8. Once mined, it will be added to the pools that you have created. As shown below, notice the UNI/ETH pair at the second-last position in the list:

Figure 21.13: Liquidity pools

9. Click on the pool to see more details, such as **Liquidity**, **Unclaimed fees**, and **Price range**:

Figure 21.14: Liquidity pool

10. You can also add more liquidity, i.e., tokens, by clicking the option **Increase Liquidity**.
11. You can also remove liquidity and close your position, and claim fees if any are earned, by clicking on **Remove Liquidity**.

In this example, we used already available tokens on the Uniswap platform, swapped ETH that we had on the Goerli network with UNI, and then created a pool using the pair. However, as the Uniswap platform is a DEX, any ERC-20 by any user can be used to create a liquidity pool.

As an exercise, can you figure out how to do this? Recall that we created the MET ERC-20 token in *Chapter 15*, *Tokenization*. Either use that same contract token or create a new one and deploy it on the Goerli test network. We already learned how to do this in *Chapter 15*, *Tokenization*. Better yet, you can also use the OpenZeppelin library to create ERC-20 tokens quite easily.

Follow the example here:
`https://docs.openzeppelin.com/contracts/4.x/erc20`. Once deployed, you can explore and confirm the deployment of the contract at Etherscan too.

Once the token contract that you created is deployed successfully, you can optionally import the token into MetaMask. After this, you can create your own liquidity pool with your own new ERC-20 token on the Uniswap platform by following the steps described earlier in this example.

With this, we complete our introduction to DeFi.

Summary

It is clear that DeFi is rapidly evolving and will continue to make a difference in our lives by providing financial services that were simply not possible before the advent of DeFi. Currently, we are witnessing the historical transformation from the internet of information into the internet of value, and as such, blockchain and DeFi will continue to make this possible. Moreover, concepts such as institutional DeFi, new types of tokens, and innovative DeFi protocols and services are going to make financial services more accessible, inclusive, tremendously efficient, and cost-effective. Use cases for private permissioned blockchains in finance and public blockchains will continue to evolve and are likely to converge at some point in the future to enable even more innovative use cases and efficiency.

Join us on Discord!

To join the Discord community for this book – where you can share feedback, ask questions to the author, and learn about new releases – follow the QR code below:

https://packt.link/ips2H