Learning Outcomes

At the end of the course, the learners will be able to be acquainted with_____

- ✓ Brief History and Introduction of Decentralized Finance (DeFi)
- ✓ Issues that Decentralized Finance (DeFi) DeFi Solves
- ✓ The infrastructure of Decentralized Finance (DeFi)
- ✓ Blockchain, Cryptocurrency
- ✓ Oracles, Stable Coins
- ✓ Primitives Techniques that DeFi May Use
- ✓ Fungible Tokens, Nonfungible Tokens
- ✓ Decentralized Finance's Key Features (DeFi)
- ✓ Lending, Derivatives, Tokenization
- ✓ Risks associated with Decentralized Finance (DeFi)
- ✓ Smart-Contract Risk, Governance Risk, Oracle Risk, Scaling Risk, and Regulatory Risk
- ✓ Salient Features of Decentralized Finance (DeFi)
- ✓ Advantages of Decentralized Finance (DeFi)
- ✓ Scopes of Decentralized Finance (DeFi)

Fundamentals of Decentralized Finance (DeFi)

Introduction

In recent years, the digital asset and cryptocurrency businesses have risen rapidly. Institutions have begun to facilitate the purchase and sale of cryptocurrencies, as well as custody services, and are now looking for new ways to participate in decentralized finance (DeFi). Digital native enterprises, venture capitalists, and people are driving the current growth in DeFi. Traditional financial institutions joining DeFi will be a watershed moment in the industry's development and progress toward universal adoption. It will have ramifications for the financial system as a whole as well as existing types of financial intermediation.

DeFi aims to change the world's present centralized financial infrastructure by adopting a decentralized internet-based architecture that depends on open-source protocols rather than traditional financial intermediaries. DeFi offers traditional financial institutions a number of development options that can improve existing operations and services – but it also poses a threat to today's financial services and business models. The way institutions react to this new kind of decentralized financial intermediation will have long-term implications for their role in the digital economy.

Module One: Overview

Lesson-01: Brief History of Decentralized Finance (DeFi)

Decentralized finance's technological foundations extend back to 2008 when the first blockchain was utilized as the distributed ledger driving bitcoin transactions, which we'll go over in more detail in the next part. However, it wasn't until a decade later that the name "DeFi" was coined. It was August of 2018, and Ethereum developers and entrepreneurs were pondering a name for the constellation of open financial applications that were being built on their blockchain. The terms "Open Horizon," "Open Financial Protocols," and "Lattice Network" was proposed, but one "DeFi" eventually won out, ushering in a worldwide, borderless, permissionless, decentralized financial revolution that is still gaining traction today.

The basic practices and concepts of DeFi are as old as humanity itself, despite the fact that the technology is relatively new. Financial transactions that are not centralized have their origins in the early barter systems and peer-to-peer exchanges, which were forerunners to the modern monetary system. Bartering is a kind of commerce in which people directly exchange goods or services for other goods or services without the use of a medium of exchange such as money. While bartering provides some advantages in some situations, it is not for everyone. When money loses value quickly, such as during hyperinflation, it has several intrinsic disadvantages. For example, in order for an exchange to take place, both parties must have what the other wants; certain items are indivisible, and so on.

Commodity money, like bartering (but not representative money), is an example of money that has value despite not being backed by the government. Commodity money is similar to today's cryptocurrencies in this regard, which are mostly unbacked and uncontrolled. Commodity money, as the name implies, gets its worth from the inherent value or use of the commodity, which might include items like salt, tea, cocoa beans, and tobacco, among others.

Compare commodity money's intrinsic value to representational money, which has no intrinsic value but represents something of value (such as gold or silver), or fiat money, whose value is derived from governmental legislation that has established it as money. As we can see from this very basic historical outline of commodity money systems, commodity-backed money, and finally fiat money, the history of the exchange of goods and services between human beings began decentralized, but morphed into our current centralized, regulated monetary system, with its national treasuries, mints, central banks, and commercial banks.

Lesson-02: Introduction of Decentralized Finance (DeFi)

Decentralized Finance (DeFi) refers to decentralized financial services offered via blockchains rather than "centralized" financial services provided by banks or other traditional financial organizations. It allows users to utilize cryptocurrencies to perform most of the functions that traditional banks can perform with government-issued fiat currencies, such as lending, borrowing, earning interest, trading assets, purchasing insurance, and so on. DeFi services are often faster, cheaper, and easier to use, with new benefits and services being added on a daily basis.

Decentralized Finance (DeFi):

Decentralized finance allows people to conduct transactions directly with other people rather than through centralized institutions such as banks, using blockchain networks. This eliminates the need for an intermediary, making financial transactions faster, cheaper, and more efficient. DeFi allows you to access your assets using secure digital wallets and transact using smart contracts. This allows you access to a variety of financial services, including peer-to-peer lending and decentralized exchange trading. Anyone with an internet connection can use DeFi, making finance significantly more accessible.

Decentralized Finance (DeFi) differs from centralized finance in the following ways:

Payments, loans, and trading activities all travel through third parties and middlemen who are extensively regulated by local regulators, making centralized finance the default financial framework in which the world currently operates. Decentralized finance, on the other hand, offers a slew of benefits by allowing users to transact through financial applications over a blockchain network, bypassing intermediaries like traditional banking organizations.

By cutting out the intermediaries, DeFi not only saves money and time but also makes financial services more accessible. Not everyone is allowed to create a bank account or have access to specific financial services in the realm of centralized finance. As a result, DeFi has the potential

to financially empower billions of individuals worldwide who currently lack access to banking services. DeFi also provides the benefit of allowing for more freedom, such as trading hours not being restricted as they are in centralized finance.

A person or group of people writing under the pseudonym Satoshi Nakamoto defined the original design and protocol for Bitcoin in his now-famous 2008 white paper Bitcoin: A Peer-to-Peer Electronic Cash System. It was a landmark moment for decentralized finance, with some now claiming that it has established two different historical points of reference for our concept of money — pre-cryptocurrency and post-cryptocurrency.

In its absolute simplicity and purposefulness, Satoshi Nakamoto's vision is a piece of beauty. More crucially, by developing a peer-to-peer network for transactions that timestamps transactions by hashing them into a continual chain of hash-based proof of work, Nakamoto shifted the scales in direction of decentralizing the existing monetary system, maybe irrevocably. The article also sets the foundation for Bitcoin's blockchain, as well as the mechanics of blockchain in general, such as cryptographic hashing, the proof-of-work process, nodes, and so on.

The story behind DeFi wouldn't be much of a story if it didn't take a quick look behind the curtain at some of the key infrastructure components, including blockchain, cryptocurrency, smart contracts (a key component of DeFi), oracles, stable coins, and decentralized applications (dApps), as well as a comparison of the Bitcoin and Ethereum blockchains.

Blockchain:

Simply said, DeFi is a system that makes financial products available to the general public via a decentralized blockchain network. A blockchain is a collection of cryptographically connected documents, or "blocks." Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. To get into a block's hash, a timestamp is now used to verify that the transaction data was there at the time the block was issued. Because each block contains information about the ones before it, they create a chain, with later blocks reinforcing previous ones.

As a result, altering blockchains can be more difficult because the recorded data cannot be changed retroactively without affecting all following blocks. To put it another way, decentralized blockchains are immutable, which means the data recorded is permanent. In general, a peer-to-peer network oversees blockchains for use as a publicly distributed ledger, with nodes following a protocol to communicate and validate new blocks.

Altcoins, Cryptocurrencies, and Stablecoins:

Bitcoin was the first DeFi application in many ways, as it allowed for decentralized money transferring over the world. The Ethereum blockchain, with its native cryptocurrency Ether, which is a transactional token that supports operations on the Ethereum network, was created in response to the constraints of the Bitcoin blockchain.

The fact that cryptocurrencies are often not issued by any central authority is one of their distinguishing features. Solana, Litecoin, and Cardano are examples of alternative currencies (altcoins) to Bitcoin. Stablecoins, on the other hand, aim to reduce or eliminate the inherent volatility of many of today's cryptocurrencies by pegging them to the US dollar or a commodity like gold. Cryptocurrencies, then, fall under the DeFi umbrella and are a key component of a new style of finance that is decentralized and devoid of central financial intermediaries.

Contracts that are smart:

Unlike the Bitcoin network, which can only be used to buy, store, and sell bitcoin, the Ethereum blockchain also has smart contracts.

Simply said, a "smart contract" is a program that runs on the Ethereum blockchain. It's a single address on the Ethereum blockchain that contains a collection of code and data. Ethereum accounts are created using smart contracts. This means they have money on their account and can send transactions across the network. They are not, however, maintained by users; instead, they are deployed to the network and run according to a set of instructions. The smart contract can then communicate with user accounts by submitting transactions that instruct it on how to execute a task. Smart contracts, like traditional contracts, can set rules that are enforced automatically by the software. Smart contracts are not deletable by default, and their interactions are irrevocable. Smart contracts are frequently compared to vending machines in that they promise a specific outcome when given the correct inputs.

ICOs:

Initial coin offerings, or ICOs, are an important part of the DeFi story since many of them have launched new blockchain projects that have had a huge impact on Ethereum and the wider crypto ecosystems. ICOs, which are essentially token sales, first gained traction in 2017 as a mechanism to sell digital assets to raise funding for blockchain-based initiatives. In 2017, an estimated $4.9 billion was raised through ICOs, making it something of a DeFi Wild West.

Initial coin offers were similar to crowdfunding operations like Kickstarter in the lack of regulatory approval systems, but the money raised was in bitcoin and Ethereum rather than dollars or Euros, and some of it just vanished (the failure rate is estimated at 47 percent). Nonetheless, a number of projects launched at the time have gone on to become top DeFi protocols, such as Aave, a platform for decentralized crypto loans with strong liquidity, and Ox, a decentralized peer-to-peer Ethereum-based token exchange.

dApps:

Decentralized applications, or "dApps," are digital applications or programs that operate on a blockchain or peer-to-peer network of computers, and are another part of the DeFi tale rather than a single computer. Peer-to-peer decentralized applications (dApps) are known to anyone who has used BitTorrent or Tor.

DApps operate in the cryptosphere on a blockchain network in a public, open-source, decentralized environment. dApps, like cryptocurrencies, exist outside of a single authority's

control. If you use the Twitter or Facebook apps, you've given over power to the companies who manage them. dApps aren't like other apps. dApps are community-driven, rather than being controlled by a single person, firm, or organization. The lack of a central authority makes them resistant to government, corporate, or individual interference, similar to cryptocurrencies.

Lesson-03: Issues that Decentralized Finance (DeFi) DeFi Solves

For millennia, we have lived in a world of centralized finance. Central banks oversee the money supply. Intermediaries are used in the majority of financial transactions. Borrowing and lending are done through traditional financial institutions. However, in recent years, significant work has been made on a quite different model: decentralized finance, or DeFi. Peers engage with peers in this system using a shared ledger that is not controlled by a single organization. DeFi has a lot of potential for addressing the five major issues with centralized finance:

- **Centralized control:**

Control is centralized. There are numerous stages to centralization. The majority of individuals and businesses work with a single, regional bank. The bank is in charge of rates and fees. It is feasible to switch, but it can be pricey. Furthermore, the banking system in the United States is heavily consolidated. Insured deposits are held by the four major banks in 44 percent of cases, up from 15 percent. Surprisingly, the banking sector in the United States is less concentrated than in other countries like the United Kingdom and Canada. A single centralized institution attempts to determine short-term interest rates and affect the rate of inflation in a centralized banking system. The phenomenon of centralization is not limited to the traditional banking industry. Certain industries are dominated by relatively new IT giants, such as Amazon (retail) and Facebook/Google (social media) (digital advertising).

- **Access is restricted:**

Unbanked people account for 1.7 billion people today, making it difficult for them to receive loans and participate in online commerce. Furthermore, many customers are forced to rely on payday lending to make ends meet. However, being banked does not ensure access. A bank, for example, might not want to bother with the tiny loan that a fledgling firm requires, and instead recommend a credit card loan. The credit card could have a borrowing rate of well over 20% per year, posing a significant barrier to discovering viable investment opportunities.

- **Inefficiency:**

There are numerous inefficiencies in a centralized financial system. The credit card interchange rate is perhaps the most egregious example since the payment network oligopoly's pricing dominance forces consumers and small companies to lose up to 3% of a transaction's value with each swipe. Fees for remittances range from 5%-7%. This seems absolutely absurd in the age of the internet. Other inefficiencies include expensive (and sluggish) capital transfers, direct and indirect brokerage costs, security issues, and the inability to execute micro transactions. Users

are often unaware of many of these inefficiencies. Because banks must cover their brick-and-mortar costs, deposit interest rates remain low and loan rates remain high under the existing banking system. In the insurance industry, a similar situation develops.

- **Lack of compatibility:**

Consumers and businesses interact with financial institutions in a disconnected world. Our financial system is compartmentalized and built to withstand large switching costs. Transferring money from one institution to another can be time-consuming and difficult. It can take three days to complete a wire transfer. This issue is well-known, and efforts are being made to address it. The attempted acquisition of Plaid by Visa in 2019 is a recent example. Plaid lets any organization with the user's authorization connect to a financial institution's information stack.

- **Lack of interoperability:**

Consumers and businesses interact with financial institutions in a disconnected world. Our financial system is compartmentalized and built to withstand large switching costs. Transferring money from one institution to another can be time-consuming and difficult. It can take three days to complete a wire transfer. This issue is well-known, and efforts are being made to address it. The attempted acquisition of Plaid by Visa in 2019 is a recent example. Plaid lets any organization with the user's authorization connect to a financial institution's information stack. This is an example of a centralized finance business attempting to acquire a product to tackle a specific problem without first addressing the underlying financial infrastructure difficulties. It was a well-thought-out strategy for gaining time.

Module Two: Infrastructure of Decentralized Finance (DeFi)

Lesson-01: Blockchain

The decentralizing backbone of everything DeFi is a blockchain. Blockchains are software protocols that allow multiple parties to function under common assumptions and data without having to trust each other. These data can include everything from the location and destination of things in a supply chain to the balances of a token's account. Updates are bundled into "blocks" and cryptographically "chained" together to allow a review of the previous history, hence the name.

A Consensus Protocol, a set of rules that decide which kind of blocks can become part of the chain and become the "truth," is the reason blockchains are possible. Up to a given security constraint, these consensus techniques are supposed to be immune to malicious tampering. The Proof of Work consensus algorithm is used by the blockchains we look at, and it relies on a computationally demanding lottery to decide which block to include. The participants agree that the truth is the longest chain of blocks. If an attacker wishes to create a longer chain including malicious transactions, they must outperform the rest of the network's computational activity.

In principle, they'd need a majority of the network's power to do so, which is why the famous 51 percent attack is considered the PoW security limit. Fortunately, amassing this much network power on the most extensively used blockchains, such as Bitcoin or Ethereum, is extremely impossible for any actor, even a whole country. Even if a majority of the network's power can be momentarily obtained, the amount of block history that can be overwritten is limited by the length of time that this majority can be maintained. While we're focusing on Proof of Work, there are a number of other consensus mechanisms to consider, the most important of which being Proof of Stake.

Validators commit some capital to verify that the block is valid under Proof of Stake. Validators stake their money to make themselves available, and then they may be chosen to propose a block. A majority of the other validators must agree on the proposed block. Validators benefit from both proposing and attesting to the validity of other people's suggested blocks. Transactions will be processed by good-faith players and appended to the ledger when a block is "won" as long as no malicious party can gain majority control of the network computational power.

Lesson-02: Cryptocurrency

Cryptocurrency is the most widely used application of blockchain technology. Cryptocurrency is a cryptographically secured and transferable token (typically scarce). Scarcity is what ensures the possibility of value, and it is a blockchain invention in and of itself. Digital items are typically easy to copy. Bitcoin is a great cryptographic feat and the potential to build something that is not duplicable in the digital realm has enormous value. Due to the asymmetric key cryptography that protects the accounts, no one can publish a fraudulent transaction without owning the matching account.

You have a "public" key for receiving tokens and a "private" key for unlocking and spending tokens that you have custody of. When you use the internet, the same type of cryptography is utilized to protect your credit card information and data. Because the ledger records an audit of their balance at any one time, a single account cannot "double-spend" their tokens because the flawed transaction would not clear. The ability to avoid "double-spend" without the need for a central authority exemplifies the major benefit of employing a blockchain to maintain the underlying ledger.

The Bitcoin blockchain is the first cryptocurrency model, and it acts almost entirely as a payment network, with the capability of storing and transacting bitcoins in real-time throughout the globe without the use of intermediaries or censorship. This is the compelling value proposition that underpins bitcoin's worth.
Despite its tremendous network effects, technology competitors provide better functionality.

Lesson-03: The Smart Contract Platform

A smart contract platform is an important component of DeFi. These blockchains go beyond simple payment networks like Bitcoin, allowing smart contracts to be created that improve the chain's capabilities. The most well-known example of a smart contract platform is Ethereum. On top of the blockchain of which it is a part, a smart contract is a code that can create and alter arbitrary data or tokens.
The idea is strong because it allows the user to quickly encode rules for any type of transaction and even create limited-edition assets with customized functionality. Many clauses in typical commercial agreements might be moved to a smart contract, which would not only enumerate but also enforce the clauses algorithmically. Smart contracts have applications in gambling, data stewardship, and supply chain management, among other things.

The existence of a transaction cost known as a gas fee is an important caveat that applies to Ethereum, but not necessarily to other smart contract systems. Consider Ethereum as a massive computer with numerous applications. Someone who wishes to utilize the computer must pay a price for each unit of calculation. A basic calculation, such as transmitting ETH, necessitates just minor changes to a few account balances. There is a minor petrol price for this. A complicated computation including the minting of tokens and the testing of numerous criteria across multiple contracts costs more gas.

An automobile is a good analogy for Ethereum. If someone wants to drive a car, they will require a specific amount of gas, which will cost money. However, the gas fee may result in a poor user experience. The gas price requires agents to keep an ETH balance in order to pay it, and they must be concerned not only about overspending, but also about underpaying and the transaction not taking place at all. As a result, efforts are underway to abstract gas prices from end-users and to assist competing chains that do away with the concept of gas entirely. However, gas is critical as a primary technique for preventing attacks on the system that result in an endless cycle of code.

It is impossible to detect malicious code of this type before it is executed, a problem known as the halting problem in computer science. By making such attacks prohibitively expensive, gas secures the Ethereum blockchain. To continue our illustration, gas solves the stopping problem as follows: Assume a "vehicle" is locked in full throttle on autopilot with no driver. Because the car must finally come to a stop when the gas tank runs out, gas functions as a limiting factor. This encourages the development of extremely efficient smart contract code, as contracts that use fewer resources and lower the likelihood of user failure have a better chance of being adopted and thriving in the market.

Lesson-04: Oracles

The fact that blockchain technologies are insulated from the world outside of their ledger is an intriguing problem. That is, the Ethereum blockchain is the only authentic source of information on what is happening on the Ethereum blockchain, not the S& P 500 index or whose team won the Super Bowl. The oracle problem is a constraint that restricts applications to Ethereum native contracts and currencies, lowering the usability of the smart contract platform.

In the context of smart contract platforms, an oracle is any data source that reports information from outside the blockchain. How can we build an oracle that can speak authoritatively about off-chain data while minimizing trust? Many applications necessitate the use of an oracle, and implementations differ in their degree of centralization.
Oracles are used in various DeFi applications in a variety of ways. An application can either host its own oracle or connect into an existing oracle from a well-trusted platform, which is a frequent approach. Chainlink is an Ethereum-based platform that uses an aggregation of data sources to solve the oracle problem.

Lesson-05: Stable Coins

Excessive volatility is a major flaw with many cryptocurrencies. This creates a barrier for customers who want to utilize DeFi apps but don't have the risk tolerance for a volatile asset like ETH. Stablecoins, a new type of cryptocurrency, have arisen to address this issue.

Stablecoins are designed to maintain price parity with a specific asset, such as the US dollar or gold. Stablecoins provide the needed stability for many DeFi applications, as well as a cryptocurrency native solution for exiting positions in more volatile crypto assets. If the target asset is not native to the underlying blockchain, it can even be used to provide on-chain exposure to the returns of an off-chain asset (e.g., gold, stocks, ETFs). The technique by which the stablecoin keeps its value changes depending on the implementation. Fiat-collateralized, crypto-collateralized, and non-collateralized stablecoins are the three main mechanisms. Fiat-collateralized stablecoins are by far the most common type. These are backed by a target asset's off-chain reserve.

Typically, these are held by an external business or set of entities that are subject to regular audits to ensure that the collateral is still present. Tether (USDT) is the largest fiat-collateralized stablecoin, with a market capitalization of $24 billion dollars, ranking third after Bitcoin and Ethereum at the time of writing.

Tether also boasts the biggest trading volume of any cryptocurrency, despite the fact that it is unaudited. USDC is the second-largest cryptocurrency, backed by Coinbase and audited by Circle. On Coinbase's exchange, USDC may be redeemed 1:1 for USD and vice versa for no cost. Due to the huge demand for stablecoin investment opportunities, USDT and USDC are particularly

popular to include in DeFi protocols. However, because these tokens are centrally controlled and have the ability to block accounts, they pose a concern.

Crypto-collateralized stablecoins are the second most common type of stablecoin. These are stablecoins that are backed by an amount of another cryptocurrency that is over collateralized. Depending on the arrangement, their value can be hard or soft tied to the underlying asset. DAI, founded by MakerDAO, is the most popular crypto-collateralized stablecoin. It is backed mostly by ETH, with collateral support for a few other crypto assets. It is soft pegged, with supply and demand incentivizing supply and demand to drive the price to $1.

Module Three: Primitives Techniques that DeFi May Use

Lesson-01: Transactions

The atoms of DeFi are Ethereum transactions. Data and/or ETH (or other tokens) are sent from one address to another in transactions. A transaction is the starting point for all Ethereum interactions, including the primitives mentioned in this section. As a result, a thorough understanding of transaction mechanics is critical to comprehending Ethereum in particular and DeFi in general.

An externally owned account (EOA) or smart contract code can be used to control addresses in Ethereum. When data is provided to a contract account, it is used to run the contract's code. The transaction may or may not include an ETH payment for the contract's use. Only ETH can be transferred via transactions submitted to an EOA. Before completing, a single transaction can interact with a large number of dApps.
The transaction begins by interacting with a single contract, which will list all of the transaction's intermediate phases in the contract body. A smart contract's clauses might cause a transaction to fail, reverting all of the transaction's previous stages; as a result, transactions are atomic. Because funds can transfer across several contracts with the knowledge and assurance that if one of the conditions is not met, the contract terms reset as if the money never left the starting point, atomicity is a fundamental property of transactions. The gas charge is relatively minimal when ETH is used to reward a miner for including and executing a transaction, for example. Longer or more data-intensive transactions are more expensive in terms of gas. If a transaction is reverted or runs out of gas for any reason, the miner loses all gas utilized up to that point. Miners are protected by forfeiture since they would otherwise be exposed to enormous amounts of failed transactions for which they would not be compensated. The market determines the gas price, which effectively establishes a bidding process for inclusion in the next Ethereum block. Higher gas taxes indicate greater demand and, as a result, are given higher priority for inclusion.

Transactions are uploaded to a memory pool, or mempool, before being included to a block, as a technical aside. Miners keep track of the transactions that have been posted, add them to their own mempools, and distribute them with other miners so that they can be included in the next available block. If the transaction's gas price is uncompetitive in comparison to other transactions

in the mempool, it is deferred to a later block. By running or connecting with mining nodes, any actor can see transactions in the mempool. This visibility can even help the miner earn from trading activities by allowing improved front-running and other competitive strategies. If a miner detects a transaction in the mempool that she can profit from by either executing it herself or front-running it, she is an incentive to do so if the block is lucky enough to win. The term miner extractable value refers to any instance of direct execution (MEV). The proof-of-work model has a flaw called MEV. Certain tactics, such as obfuscating transactions, can reduce MEV by disguising how miners might profit from the transactions from miners.

Lesson-02: Fungible Tokens

The value proposition of Ethereum and DeFi is built around fungible tokens. Any Ethereum developer can design a token with units that are all equal and interchangeable and is divisible to a particular decimal granularity. For example, one $100 dollar is equal to one hundred $1 bills, making USD a fungible asset. ERC-20 is the Ethereum blockchain token interface. From the standpoint of an application developer, an interface is the bare minimum of functionality. When a coin implements the ERC-20 interface, any application that handles the stated functions generically can integrate with the token instantaneously and effortlessly. Application developers can securely support coins that do not yet exist using ERC-20 and related APIs. An ERC-20 coin can be in multiple categories at the same time.

- **Equity Token:**

An equity token is a token that reflects ownership of an underlying asset or pool of assets. It is not to be confused with equities or stocks in the traditional financial sense. The units must be fungible, which means they must all correspond to the same share of the pool. Assume that a token, TKN, has a total fixed quantity of 10,000 and that TKN equates to a 100-ETH Ethereum pool stored in a smart contract. The smart contract says that it will refund a pro-rata amount of ETH for each unit of TKN it gets, setting the exchange rate at 100 TKN/1 ETH.

We may extend the example to include a variable amount of ETH in the pool. Assume that the pool's ETH grows at a rate of 5% per year due to some other mechanism. Now, 100 TKN is equal to 1 ETH + a 5% ETH cash flow in perpetuity. This information can be used by the market to appropriately price TKN.

The pools of assets in true equity tokens can have considerably more sophisticated mechanisms than a static pool or predetermined rates of increase. Only what can be encoded into a smart contract limits the possibilities.

- **Utility Tokens:**

Utility tokens are a catch-all category in many ways, yet they do have a precise definition. Utility tokens are fungible tokens that are required to use certain smart contract system functionality or have an intrinsic value proposition established by the smart contract system in question.

Utility tokens drive the economics of a system in many circumstances, producing scarcity or incentives where the developers intended. Utility tokens allow systems to accumulate and retain the economic value that is not linked to Ethereum as a whole. While ETH might be used in some circumstances instead of a utility token, utility tokens allow systems to accumulate and maintain decoupled economic value from Ethereum as a whole. A system with an algorithmically varied supply is an example of a use case that necessitates a distinct utility token.

Regardless of whether the stablecoin is fiat collateralized, crypto-collateralized, or algorithmic, the last example applies to all stablecoins. The utility token in USDC, a fiat-collateralized stablecoin, functions as its own system, with no additional smart-contract infrastructure to support its value. The guarantee of redemption for USD by its backing firms, including Coinbase, gives USDC its value. Utility tokens have far more applications than the few we've discussed here.

As new economic and technological mechanisms arise, this category will increase.

- **Governance Tokens:**

In the same way that equity tokens represent percentage ownership, governance tokens do as well. Governance token ownership, rather than asset ownership, refers to voting rights, as the name implies. We begin by motivating owners to vote on the types of changes they want to see.

Many smart contracts include provisions that specify how the system might change; for example, permitted changes could include tweaking parameters, adding new components, or even changing the functionality of current components. Given the likelihood that the contract with which a user interacts today may change tomorrow, the system's flexibility to evolve is a powerful offer. Only developer admins who have encoded special privileges for themselves can govern changes to the platform in some situations. Because of the admins' centralized control, any platform with admin-controlled features is not truly DeFi. However, a contract that lacks the ability to alter is bound to be rigid, as it has no way of adapting to defects in the code or changing economic or technical conditions. As a result, many systems aspire towards a decentralized upgrade process, which is frequently facilitated by a governance token.

Lesson-03: Nonfungible Tokens

NFT Standard:

The ERC-721 standard on Ethereum defines nonfungibility. This standard is identical to ERC-20, except that instead of all units being recorded as a single balance, each unit has its own unique ID. This one-of-a-kind identifier can be linked to additional metadata that distinguishes the token from others issued under the same contract. The balance method returns the total quantity of nonfungible tokens (NFTs) that the address holds in the provided contract. A further method, the owner, returns a specific token that the address owns and is identified by its ID. Another significant distinction is that ERC-20 allows for partial approval of an operator's token holdings, but ERC-721 is all-or-nothing. Any of the NFTs can be moved by an operator who has been allowed to utilize them.

In DeFi, NFTs have a lot of potentials. Their other name, deeds, suggests that they are used to symbolize unique ownership of unitary assets, such as ownership of a specific P2P loan with its own rates and terms.
Using the ERC-721 interface, the item may then be transferred and sold. Another application could be to represent a lottery stake. Lottery tickets may be called nonfungible since only one or a small number of them will be winners, leaving the rest worthless. NFTs also have a strong use case in their capacity to employ collectibles to bridge financial and non-financial use cases. NFTs can also represent scarce items in a game or other network, with secondary marketplaces for NFTs retaining economic value.

Multi-Token Standard:
Individual contracts and addresses are required for ERC-20 and ERC-721 coins to be deployed on the blockchain. These requirements can be difficult to meet in systems with a large number of closely related tokens, possibly even a mix of fungible and nonfungible token types. The ERC-1155 token standard tackles this problem by proposing a multi-token paradigm in which the contract maintains balances for a variable number of fungible or nonfungible tokens. Batch reading and transfers are also supported by the standard, which reduces gas costs and improves user experience. Operators are approved for all supported tokens in a binary all-or-none fashion under ERC-1155, similar to ERC-721.

Module Four: Decentralized Finance's Key Features (DeFi)

Lesson-01: Lending

MakerDAO (decentralized autonomous organization) is frequently cited as a DeFi exemplar. There must be a foundation for a series of applications to build on top of one another. MakerDAO's main value proposition is the establishment of a crypto-collateralized stablecoin tied to the US dollar. This means that the system can run entirely on the Ethereum blockchain, without the need for external centralized organizations to back, vault, or audit the stablecoin. MakerDAO is a two-token paradigm in which a governance token, MKR, grants voting rights and participates in value capture on the platform. The second token is the DAI stablecoin, which is a key component of the DeFi ecosystem and is used by a number of protocols.

- **Compound:**

The compound is a lending market that allows you to borrow and lend a variety of ERC-20 assets. Every lender receives the same variable rate, and every borrower pays the same variable rate because all the tokens in a particular market are pooled together. The concept of a credit score is useless, and due to the anonymity of Ethereum accounts, ensuring repayment in the case of loan default is very difficult. As a result, all loans are over-collateralized in a different collateral asset than the one being borrowed. If a borrower's collateralization ratio falls below a certain level, their position is liquidated to pay off their loan. A keeper can liquidate the debt in the same

way as MakerDAO Vaults does. For each unit of debt that is paid off, the keeper receives a bonus incentive.

A collateral factor is used to compute the collateralization ratio. On the platform, each ERC-20 asset has its own collateral component, which ranges from 0% to 90%. An asset with a 0 collateral element cannot be utilized as collateral. For a single collateral type, the required collateralization ratio is 100 divided by the collateral factor. Volatile assets have lower collateral factors, which necessitate greater collateralization ratios due to the increased risk of under collateralization from a price fluctuation. When numerous collateral kinds are used simultaneously in a portfolio, the collateralization ratio is calculated as 100 divided by the weighted average of the collateral types by their relative sizes.

- **Aave:**

Aave (which was launched in 2017) is a loan market protocol that is similar to Compound but has a few more capabilities. Aave, in addition to Compound, offers a large number of additional tokens to supply and borrow. The compound now offers eight different tokens (various ERC20 Ethereum-based assets), while Aave offers these eight plus nine additional tokens not available on Compound. Importantly, the Aave loan and variable borrowing rates are more predictable, as there is no subsidy involved, unlike the unpredictable COMP token in Compound. The Aave protocol encourages the creation of wholly new marketplaces. Each market has its own set of token pools, each with its own supply and borrowing interest rates. The advantage of creating a distinct market is that the market's supported tokens can only be used in that market and cannot be used in other markets, reducing the risk of contagion.

Lesson-02: Derivatives

- **Yield Protocol:**

Yield Protocol presents a derivative model for zero-coupon bonds that are secured. A yToken is an ERC-20 (fungible) token that settles in a defined quantity of a target asset at a given date, according to the protocol. The contract will state that fungible tokens are those that have the same expiration date, target asset, collateral asset, and collateralization ratio. The tokens are backed by the collateral asset and have a needed maintenance collateralization ratio, similar to MakerDAO and other DeFi platforms we've looked at. If the value of the collateral falls below the required level of maintenance, the position can be liquidated by selling some or all of the collateral to cover the obligation. The process for yToken settlement is still up in the air, however, one option is "cash" settlement, which entails paying an equivalent amount of the collateral asset worth the target asset's stipulated amount.

- **Synthetix:**

There is a decentralized alternative to many classic derivative products. DeFi, on the other hand, thanks to smart contracts, allows for new sorts of derivatives. Synthetix is working on a brand-new derivative. Consider developing a derivative cryptoasset whose value is based on a non-owned and non-escrowed underlying asset. Synthetix is a company whose main goal is to develop a wide range of liquid synthetic derivatives. At a high level, its model is simple and original. The company issues Synths, which are backed by collateral and whose prices are tied to an underlying price feed. DAI, MakerDAO's synthetic asset, is likewise a synthetic asset. The Chainlink's decentralized oracles.29 provide the pricing feeds. Synths may theoretically track any asset, including long and short, as well as leveraged positions. There is no leverage in practice, and the key assets tracked are cryptocurrencies, fiat currencies, and gold.

Lesson-03: Tokenization

Tokenization is the process of taking an asset or a group of assets, either on or off the blockchain, and either

1. reflecting that asset on the blockchain with fractional ownership, or
2. producing a composite token that holds a number of underlying tokens.

A token can adhere to a variety of standards depending on the type of features a user desire. As previously said, the most widely used token standard is ERC-20, which is a fungible token standard. This interface abstractly defines how a token with non-unique and replaceable units (such as USD) should function. The ERC-721 standard, which defines nonfungible tokens, is another option (NFTs). These tokens are one-of-a-kinds, such as a token that represents ownership of a work of art or a specific digital asset from a video game. These and other standards can be used by DeFi applications to support any token that uses the standard by just coding for the single standard.

Set Protocol:

The "composite token" approach to tokenization is used by Set Protocol. Set Protocol mixes Ethereum tokens into composite tokens that act more like traditional exchange-traded funds, rather than tokenizing assets that aren't native to Ethereum (ETFs). Set Protocol integrates crypto assets into Sets, which are ERC-20 tokens that are fully collateralized by the smart contract components. A Set token can always be redeemed for its parts. Based on a trading strategy, sets might be static or dynamic. Static Sets are simple to comprehend and consist of packaged tokens that the investor is interested in; the resulting Set can be transferred as a single unit.

Dynamic Sets are a type of trading technique that governs when and how reallocations can be made. For example, anytime ETH crosses its X-day simple or exponentially weighted moving average, the "Moving Average" Sets move between 100 percent ETH and 100 percent USDC. These Set coins, like traditional ETFs, contain fees and sometimes performance-related

incentives. The fees are pre-programmed by the manager when the Set is created, and they are paid directly to the manager for that specific Set. A buy fee (front-end load cost), a streaming fee (management fee), and a performance fee are the three fee alternatives offered (percentage of profits over a high-water mark). The Set Protocol does not now charge a fee, but it may do so in the future. Set Protocol's pricing and returns are calculated using MakerDAOs' publicly available oracle price feeds, which Synthetix also uses.

The key benefit of dynamic Sets is that the trading strategies are openly encoded in a smart contract, allowing customers can see exactly how their assets are being allocated and simply redeem their funds at any time. Set Protocol also offers a Social Trading function, which allows a user to buy a Set whose portfolio is limited to specific assets and whose reallocations are controlled by a single trader. These portfolios are more like mutual funds because they are actively managed. The advantages are similar in that the portfolio manager has a predetermined set of assets from which to choose, and the users benefit from the contract-enforced asset allocation.

Module Five: Risks associated with Decentralized Finance (DeFi)

Lesson-01: Smart-Contract Risk

Crypto-focused products, especially exchanges, have been regularly hacked over the last decade. While many of these attacks were the result of inadequate security measures, they nevertheless highlight an essential point: software is particularly vulnerable to hacks and developer errors. With their unique qualities, blockchains can eliminate traditional financial problems like counterparty risk, yet DeFi is based on code. This software base provides attackers with a greater attack surface than typical financial institution threat vectors. Public blockchains, as previously said, are open platforms. Following the deployment of code on a blockchain, anyone can examine and interact with it. Because this code is frequently in charge of keeping and moving blockchain native financial assets, it poses a new and distinct danger. Smart contract risk is the name given to this new attack vector.

DeFi is built on a smart contract, which is a type of public computer code. While Nick Szabo first proposed the concept of a smart contract in a 1997 paper, the implementation is new to mainstream engineering practice. As a result, formal engineering approaches for reducing the risk of smart contract defects and programming errors are still in the works. A logic fault in the code or an economic exploit in which an attacker can remove funds from the platform beyond the intended functionality are both examples of Smart Contract risk. The former can take the shape of any standard software flaw. Let's imagine we build a smart contract that is designed to escrow deposits from any user into a specific ERC-20 and then transfers the full balance to the lottery winner. Internally, the contract maintains track of how many tokens it has and uses that number as the amount when transferring funds. In our hypothetical contract, the defect will fit right in. Due to a rounding issue, the internal figure will be slightly greater than the actual token balance held by the contract. When it tries to transmit, it will do so "in excess," causing the

execution to fail. The tokens are functionally locked within the protocol if there is no failsafe in place. This money is referred to as "bricked" informally and cannot be recovered. An economic ruse would be more deceptive. There would be no clear flaw in the logic of the code, but rather an opportunity for an economically powerful enemy to manipulate market conditions in order to profit improperly at the expense of the contract. Consider the case where a contract serves as trade between two tokens. It decides the price by comparing it to the exchange rate of another identical contract on the chain and offering it with a little adjustment.

Lesson-02: Governance Risk

Risks in programming are nothing new. They've been around for more than half a century, dating back to the start of modern computing. Because the application is autonomous and regulated by smart contracts, programming risk is the only concern to some protocols, such as Uniswap. Other DeFi applications rely on more than just computer code that runs on its own. MakerDAO, the previously mentioned decentralized credit facility, relies on a human-controlled governance process that actively alters protocol parameters to keep the system solvent. Many additional DeFi protocols rely on humans to actively manage protocol risk, and many of them utilize similar approaches. This creates a new risk, governance risk, that is specific to the DeFi environment. The representational or liquid democratic processes that permit protocol alterations are referred to as protocol governance. Users and investors must purchase a token on a liquid marketplace that has been explicitly allocated protocol governance rights in order to participate in the governance process. Holders of these tokens can use them to vote on protocol improvements and help shape the future. Although governance tokens typically have a set supply, which helps to prevent attempts by anybody to get a majority (51 percent), they nevertheless expose the protocol to the possibility of being taken over by a hostile actor.

While we have yet to witness a serious governance attack in action, new projects like Automata38 allow users to directly purchase governance votes, increasing the potential of malicious/hostile governance. Traditional fintech companies are frequently controlled by their founders, which lessens the danger of an outside party influencing or changing the company's direction or product. However, as soon as the governance system is live, DeFi protocols become vulnerable to assault. Any well-funded enemy can simply buy a majority of the liquid governance tokens to take control of the protocol and steal cash.

Lesson-03: Oracle Risk

Oracles are one of the final unsolved challenges in DeFi, and most DeFi protocols require them to work properly. Oracles are designed to answer a basic question: how can off-chain data be securely relayed on the blockchain? Blockchains without oracles are totally self-contained, with no awareness of the outside world other than the transactions added to the native blockchain.

To ensure that routine procedures like liquidations and prediction market resolutions work properly, several DeFi protocols require access to secure, tamper-resistant asset pricing. The use of these data streams as a protocol adds oracle risk.

Oracles pose a huge threat to the systems they assist. If the Cost of Corruption of an oracle is ever less than the possible Profit from the Corruption of an attacker, the oracle is particularly vulnerable to attack. There have been three types of oracle solutions invented, developed, and used to date. A Schelling-point oracle is the first. The owners of a fixed-supply token vote on the outcome of an event or report the price of an asset in this oracle. Augur and UMA are examples of this type of oracle. While Schelling-point oracles maintain the decentralization of protocols that rely on them, they have long resolution times. The API oracle is the second sort of Oracle solution. These oracles are centralized entities that reply to data or price requests asynchronously. Provable, Oraclize, and Chainlink are some examples. All systems that rely on API-based oracles must trust the data provider to answer all requests correctly. A tailored, application-specific oracle service is the third form of oracle. Maker and Compound both employ this form of oracle. Its design varies depending on the protocol needs for which it was created. To send all on-chain price data to the Compound oracle, for example, Compound relies on a single data provider that the Compound team controls. Oracles, in their current state, pose the greatest threat to DeFi protocols that rely on them. All onchain oracles are subject to front-running, and arbitrageurs have cost millions of dollars. Furthermore, oracle services such as Chainlink and Maker have experienced crippling outages with disastrous consequences. Oracles pose the greatest systemic threat to DeFi today unless they are blockchain native, hardened, and proven resilient.

Lesson-04: Scaling Risk

Ethereum and other "Proof of Work" (consensus mechanism) blockchains have a fixed block size, as we've seen. Every Ethereum miner must run all of the included transactions on their equipment for a block to become part of the chain. It is impractical to expect each miner to execute all financial transactions for a global financial market. Ethereum currently has a maximum transaction rate of 15 TPS. Despite this, this blockchain now houses practically all of DeFi. Ethereum can only manage less than 0.1 percent of the throughput of Visa, which can handle up to 65,000 transactions per second. DeFi is at risk of not being able to meet demand due to Ethereum's lack of scalability. Much work is being put into improving Ethereum's scalability or replacing it with a blockchain that can manage bigger transaction volumes more easily. To date, all attempts to help Ethereum have failed. New systems such as Polkadot, Zilliqa, and Algorand, on the other hand, offer some solutions to this scaling issue.

Proof of Stake, a novel consensus algorithm, is one actively explored solution to the problem. Proof of Stake simply substitutes staking an asset on the next block for block mining (which involves a probabilistic wait time), with majority rules identical to PoW. A user escrows assets in a smart contract and is susceptible to a penalty (slashed funds) if they stray from expected conduct, which is an important idea in cryptocurrencies and DeFi. Voting for numerous candidate

blocks is an example of harmful activity in Proof of Stake. This conduct is penalized since it demonstrates a lack of discernment and skews voting counts. Proof of Stake's security is built on the idea that a malicious actor would have to amass more of the staked asset (either in the case of Ethereum) than the entire chain's stakes. Due to the impossibility of achieving this goal, significant security features equivalent to PoW are obtained.

Lesson-05: Regulatory Risk

As the DeFi market grows in size and importance, it will be scrutinized by regulators more closely. Previously disregarded by the CFTC, major centralized spot and derivatives exchanges have suddenly been obliged to comply with KYC/AML compliance directives, and DEXs appear to be next. Several decentralized derivatives exchanges, such as dYdX, have already had to geoblock US consumers from using certain exchange features. While the noncustodial and decentralized structure of DEXs creates a legal grey area with an unknown regulatory future, there is little question that once the market grows, regulation will follow. Due to legal issues, the well-known algorithmic stablecoin project Basis was forced to suspend in December of 2018. Unfortunately, the requirement to implement US securities regulations to the system hampered our ability to launch Basis. As a result, I'm sorry to inform you that we've decided to return funds to our investors. Unfortunately, this also means that the Basis project will be shut down. DeFi has seen an increase in the number of anonymous protocol founders in response to regulatory pressure. An unidentified group forked the original Basis project earlier this year. Governance tokens, which have been published by a number of DeFi initiatives, are also attracting more attention as the SEC considers whether these new assets may be classified as securities.

Module Six: Salient Features of Decentralized Finance (DeFi)

Lesson-01: Features of Decentralized Finance (DeFi)

The majority of financial services have a decentralized counterpart. Ethereum, on the other hand, allows for the creation of whole new financial instruments. This is an ever-expanding list.

- **Send money around the globe quickly:**

Ethereum was created as a blockchain to send transactions in a safe and worldwide manner. Ethereum, like Bitcoin, makes transmitting payments throughout the world as simple as sending an email. Simply enter your recipient's ENS name or wallet account address, and your funds will be forwarded to them in seconds. To send and receive payments, you'll need a wallet. Ethereum can be used to send money as well. This allows you to pay someone their salary every second, giving them instant access to their money. You can also rent something by the second, such as a storage locker or an electric scooter. If you don't want to send or stream ETH because of its volatile value, there are stablecoins, which are Ethereum-based substitute currencies.

- **Access stable currencies:**

Volatility in cryptocurrencies is an issue for many financial products and everyday spending. Stablecoins have been used by the DeFi community to solve this problem. Their value is fixed against another asset, usually a popular currency such as the US dollar. The value of Dai and USDC coins is only a few pennies short of a dollar. As a result, they're great for both earning and selling. Many Latin Americans have used stablecoins to protect their valuables at a period when their government-issued currencies were extremely volatile.

- **Borrowing with privacy:**

Nowadays, everything revolves around the people who give and borrow money. Before lending money, banks want to know if you'll be able to repay it. It is not necessary for either party to divulge their identity when using decentralized lending. Instead, the debtor must put up security, which will be transferred to the lender immediately if the loan is not repaid. Some lenders will even take NFTs as security. A deed to a one-of-a-kind item, such as a painting, is referred to as a non-transferable title (NFT). This allows you to borrow money without submitting any personal information or having your credit checked.

- **Tax-efficiencies:**

Borrowing permits, you to get the money you need without having to sell any of your ETH. ETH, on the other hand, can be used as security for a stablecoin loan. This provides you with the funds you require while allowing you to keep your ETH. Stablecoins, unlike ETH, do not fluctuate in value and are hence favored when cash is required.

- **Flash loans:**

Flash loans are a type of decentralized lending that allows you to borrow money without having to put up any collateral or provide any personal information. They are currently inaccessible to non-technical individuals, but they hint at what might be possible for everyone in the future. It is based on the concept of simultaneously borrowing and repaying a loan. The transaction is handled as if it never happened if it is not repaid. Liquidity pools are places where money is kept that is often used. Someone can borrow them, do business with them, and pay them back in full at the same time they were borrowed if they aren't being used at the time. In a highly personalized transaction, this needs a large degree of thinking. A simple example is someone who uses a flash loan to borrow as much of an asset at one price in order to sell it in a different market for a higher price.

Lesson-02: Advantages of Decentralized Finance (DeFi)

Decentralized finance uses the Ethereum blockchain's key principles to improve financial security and transparency, open liquidity and development potential, and promote a unified and uniform economic system.

- **Programmability:**

Smart contracts with a high level of programmability automate execution and allow the creation of new financial instruments and digital assets.

- **Immutability:**

Data coordination across a blockchain's decentralized architecture is tamper-proof, which improves security and audibility.

- **Touching:**

Ethereum's composable software design allows DeFi protocols and apps to integrate and complement one another. Developers and product teams can construct interfaces and integrate third-party applications with DeFi by building on top of existing protocols.

- **Transparency:**

Every transaction on the public Ethereum blockchain is broadcast to the Ethereum network and confirmed by other users. This level of transaction data transparency not only allows for comprehensive data analysis, but also ensures that all users can see network activity. Ethereum and the DeFi protocols that run on it are both open-source projects that anybody can look at, and audit, and improve.

- **Permission less:**

DeFi, in contrast to traditional finance, is distinguished by its open, permission-less access. Regardless of their location or financial situation, anyone with a virtual wallet and Internet access can use Ethereum-based DeFi applications.

- **Self-Custody:**

DeFi market participants always preserve custody of their assets and control of their personal data by interacting with permission-fewer financial applications and protocols utilizing Web3 wallets like MetaMask.

Lesson-03: Scopes of Decentralized Finance (DeFi)

Decentralized financial protocols have opened up a world of new economic activity and opportunities for people all around the world, from DAOs to synthetic assets. DeFi is much more than an emerging ecosystem of projects, as evidenced by the extensive list of use cases below. Rather, it's a large, well-coordinated effort to build an Ethereum-based alternative financial system that can compete with centralized services in terms of accessibility, robustness, and clarity.

- **KYC (Know Your Customer):**

Know-your-customer (KYC) guidelines are used in traditional finance to ensure anti-money laundering (AML) and counter-terrorist financing (CFT) compliance. Ethereum's decentralized infrastructure allows for next-generation compliance analysis based on the behavior of participating addresses rather than participant identities in the DeFi space. This know-your-transaction (KYT) service, such as those offered by MetaMask Institutional, assist in the real-time assessment of risk and the prevention of fraud and financial crimes.

- **DAOs:**

A Decentralized Autonomous Organization (DAO) is a decentralized autonomous organization that cooperates according to transparent rules inscribed on the Ethereum blockchain, removing the need for a centralized administrative agency. Maker and Compound, two popular DeFi protocols, have developed DAOs to collect funds, run financial operations, and decentralize governance to the community.

- **Data and analytics:**

DeFi protocols offer significant advantages for data discovery, analysis, and decision-making around financial opportunities and risk management due to their extraordinary transparency around transaction data and network activities. DeFi Pulse is one of many tools and dashboards that enable customers to track the value locked in DeFi protocols, measure platform risk, and compare yield and liquidity.

- **Derivatives:**

Smart contracts based on Ethereum allow for the construction of tokenized derivatives whose value is generated from the performance of an underlying asset and where counterparty agreements are hardcoded in code. DeFi derivatives can reflect both real-world assets and cryptocurrencies, such as fiat currencies, bonds, and commodities.

- **Insurance:**

DeFi is still a relatively new concept, and smart contract flaws and breaches pose hazards.

Customers can now choose from a choice of new insurance options to help them get coverage and preserve their investments. For example, Nexus Mutual offers a Smart Contract Cover that protects against unintended smart contract code usage.

- **Marketplaces:**

DeFi protocols are enabling a plethora of online markets that allow users to trade things and services globally and peer-to-peer—everything from freelance coding assignments to digital collectibles to physical jewelry and garments.

- **Payments**

Peer-to-peer payment is likely the most fundamental use case for DeFi and the blockchain ecosystem in general. Users can exchange cryptocurrencies securely and directly with one another using blockchain technology, which eliminates the need for middlemen. DeFi payment systems assist large financial institutions to optimize market infrastructure and better serving wholesale and retail customers, resulting in a more open economic system for underbanked and unbanked people.

Conclusion

The need for robust regulation is crucial as the DeFi industry continues to grow and exist as an alternative financial system to traditional finance. To facilitate the credibility of DeFi systems, they would need to comply with AML-KYC regulations and manage the financial stability risk associated with the use of stablecoins, as mentioned above. DeFi must be governed in a way that is consistent with the technology's operation. Because of the technology's distinctiveness, DeFi protocols would need to include regulation. This could entail including KYC requirements into the protocol itself, as well as requiring the protocol to verify that a stablecoin is backed by a digital currency counterpart issued by a central bank. The technology's uniqueness would necessitate collaboration among software developers, investors (such as DeFi governance token holders), regulators, and industry experts. Regulators would also need to learn software programming abilities in order to certify protocols/codes as compliant. In order to build a viable framework for regulating DeFi, all of these aspects must be taken into account.

Fundamentals of Decentralized Finance (DeFi)

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

About Your

Joseph Holbrook, CLO of Techcommanders in Jacksonville, FL

- Certified Blockchain Solutions Architect (CBSA)
- Certified Google Cloud Platform Cloud Architect
- Certified AWS Solutions Architect
- FinOps Practitioner
- Brocade Distinguished Architect (BDA) 2013
- EMC Proven Professional – Expert – Cloud (EMCCE)
- Published Course Author on Pearson Safari, Udemy, LinkedIn Learning
- Published Book Author – Architecting Enterprise Blockchain Solutions
- CompTIA Subject Matter Expert, SME
- Prior US Navy Veteran

TECH COMMANDERS
ADVANCING YOUR IT SKILLS

What is Decentralized Finance?

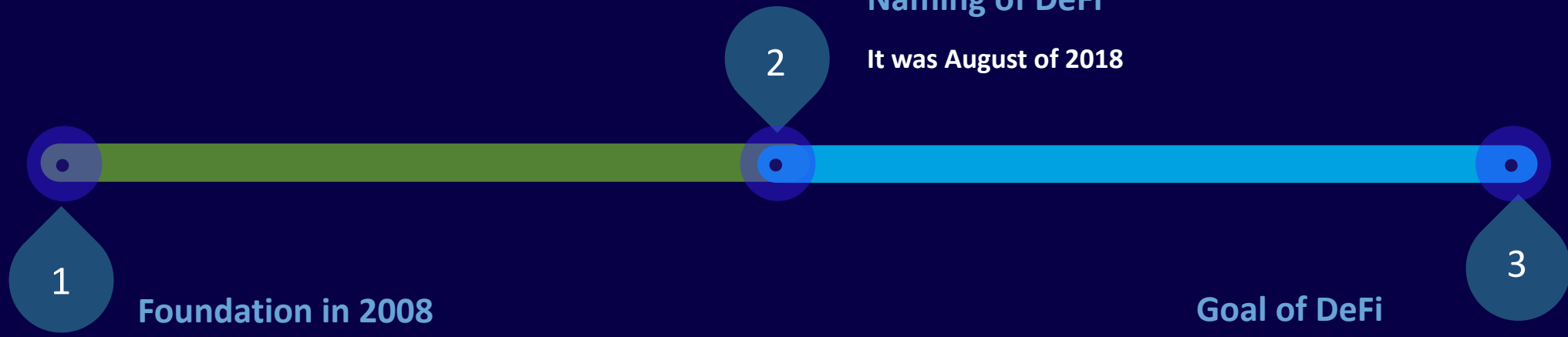
A new type of financial system which is based on secure blockchains similar to those used by cryptocurrencies.

Primary Features of DeFi:

- It does away with the usage fees that banks and other financial institutions impose.
- Instead of depositing your money in a bank, you keep it in a secure digital wallet.
- It can be used by anyone with an internet connection without authorization.
- Fund transfers can be completed in seconds or minutes.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

History of Decentralized Finance (DeFi)



Naming of DeFi

It was August of 2018

Foundation in 2008

Decentralized finance's technological foundations extend back to 2008 when the first blockchain was utilized as the distributed ledger driving bitcoin transactions.

Goal of DeFi

The goal of DeFi is to get rid of the third parties that are involved in all financial transactions.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Centralized Vs Decentralized Finance

Centralized Finance

A type of financial practice where users can borrow money and receive interest on their digital assets, such as Bitcoin, Ethereum, USD Coins like USDT & USDC, and so on, through a centralized platform.

Decentralized Finance

Automated contracts don't need banks or intermediaries to be executed. They employ blockchain technology and function on the Ethereum network. The money is not accessible to any business or person.

Difference Between CeFi and DeFi

Centralized finance

1. Trading activities all travel through third parties.
2. Not accessible to everyone.
3. Gives flexibility in converting from fiat to cryptocurrencies and vice versa.
4. User's fund custody is under the third party.

Decentralized finance

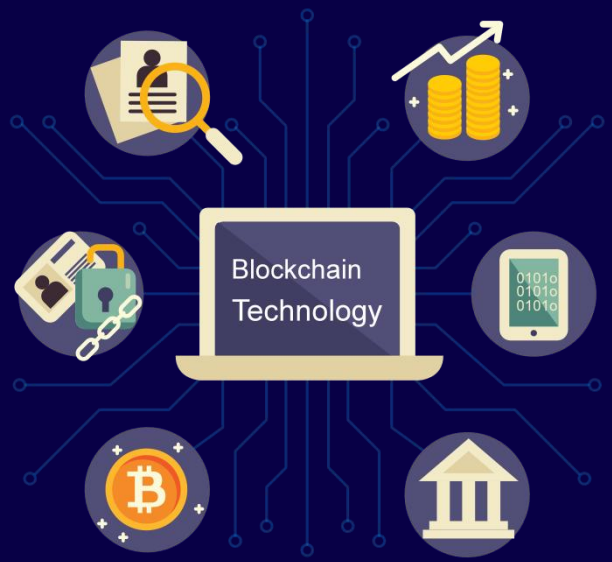
1. Transections through financial applications over a blockchain network.
2. More financially accessible and with the potential of financial inclusion for billions of individuals worldwide.
3. DeFi services do not provide fiat with as much flexibility as centralized entities.
4. Here, the user has total control over the handling of funds.

The key infrastructural components of DeFi

1

Blockchain

Blockchain is a method of storing data that makes it challenging or impossible to alter, hack, or defraud the system.



2

Cryptocurrency

An encrypted data string that indicates a unit of currencies like Bitcoin, Solana, Litecoin, and Cardano .

3

Smart Contracts

A program that running on the Ethereum blockchain and containing a collection of code and data

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Other key infrastructural components of DeFi

1

ICOs

initial coin offerings (ICOs) is as like Initial public offerings (IPOs) in the share market to raise funds.

1

dApps

Digital applications or programs that operate on a blockchain or peer-to-peer network of computers.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Issues that Decentralized Finance Solves

1

Centralized control

Control is centralized. The bank is in charge of rates and fees.

Access is restricted

Unbanked people account for 1.7 billion people today. Financial inclusion can be raised by DeFi system.

2

3

Inefficiency and Costly

Consumers and small companies have to lose up to 3% of a transaction's value with each swipe.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Issues that Decentralized Finance Solves

4

Lack of interoperability

Transferring money from one institution to another can be time-consuming and difficult.

5

Documentation Barrier

The consumers have to face a number of hustles because of documentation like KYC, Know Your Customer, form.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Blockchain Technology

Blockchain is a type of shared database that differs from traditional databases in the way it is stored: data is stored in blocks, which are then connected via cryptography.

Types of Blockchain

01

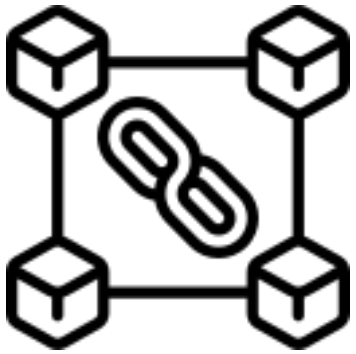
Private Blockchain Networks

Private blockchains are ideal for private businesses and organizations

02

Public Blockchain Networks

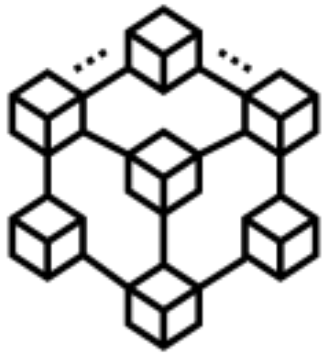
They popularize distributed ledger technology, gave birth to Bitcoin and other cryptocurrencies (DLT)



03

Permissioned Blockchain Networks

These types of blockchains are commonly set up by businesses to obtain the best of both worlds



04

Consortium Blockchains

They can provide more security once they are up and running as well as well-suited to multi-organization collaboration.

Introduction to Cryptocurrency

1. Decentralized (No Central Authority)
2. Irreversible and Immutable (Cannot be Undone)
3. Anonymous
4. Limited Supply and Scarcity

Cryptocurrency Exchanges: Buying and Selling Basics

Types of Cryptocurrency Exchanges

Working Process of Crypto Wallets

Types of Crypto Wallets

Crypto Coin & Token

TECH COMMANDERS
ADVANCING YOUR IT SKILLS

Steps to Start Investing in cryptocurrency

Step-1

Decide whether you want to buy or trade

Step-2

Decide which currencies you want to buy and sell

Step-3

Decide on your trading strategy

Step-4

Choose the best crypto exchange

Step-5

Create an account with a trading platform

Step-6

Add money to your account

Step-7

Investing and buying cryptocurrency

Step-8

Put your cryptocurrency in a safe place

Step-9

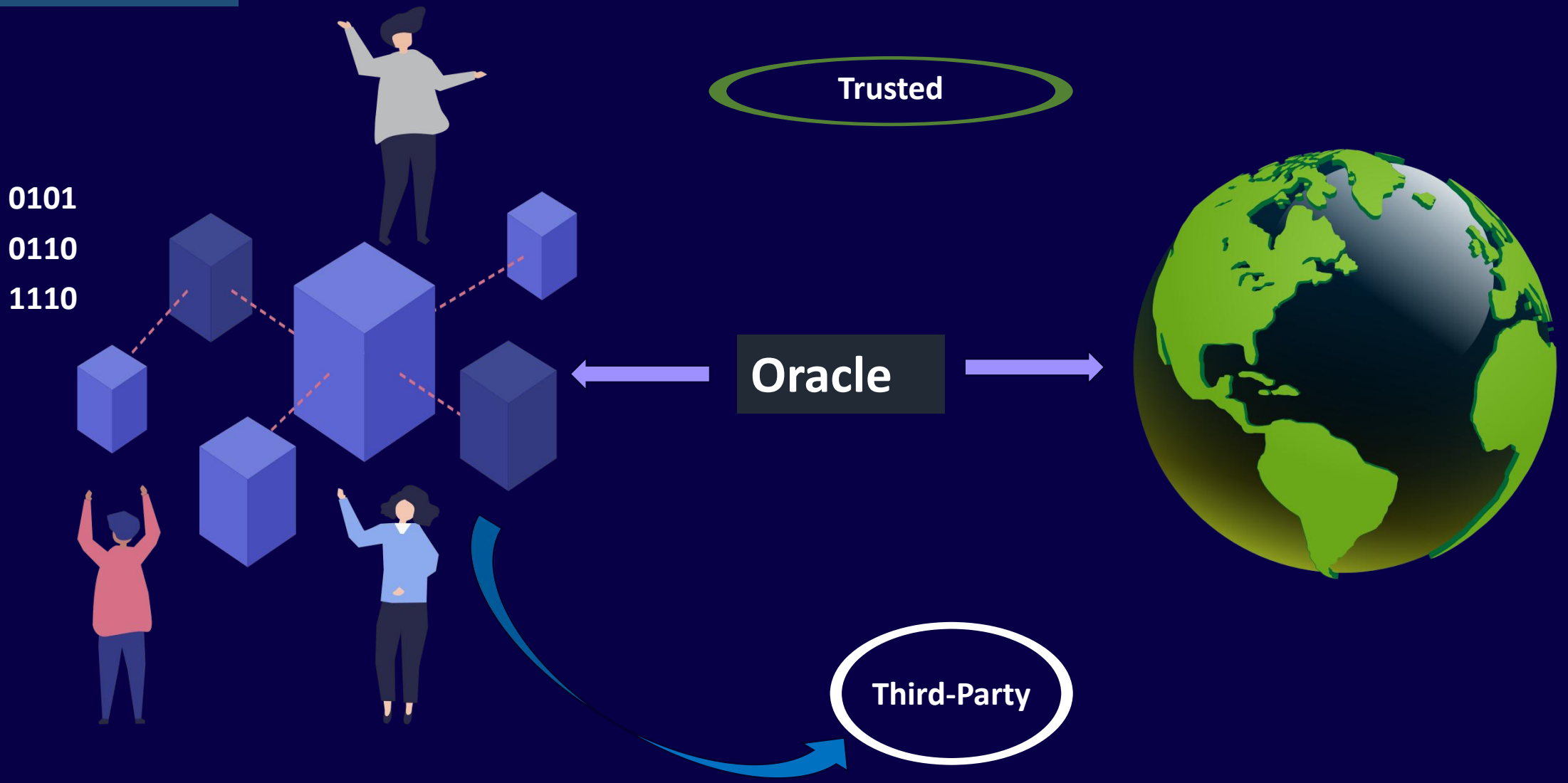
Decide on a plan of action

The Smart Contract Platform

- Smart contracts are the agreements on blockchain that get executed if the agreements are met.
- Actually, they are just like contracts in the real world. Here, the difference is that they are done digitally.
- The most well-known example of a smart contract platform is Ethereum.

Oracles

An oracle is a trusted third party that gives you reliable data outside the current information that you have access to see back.



TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

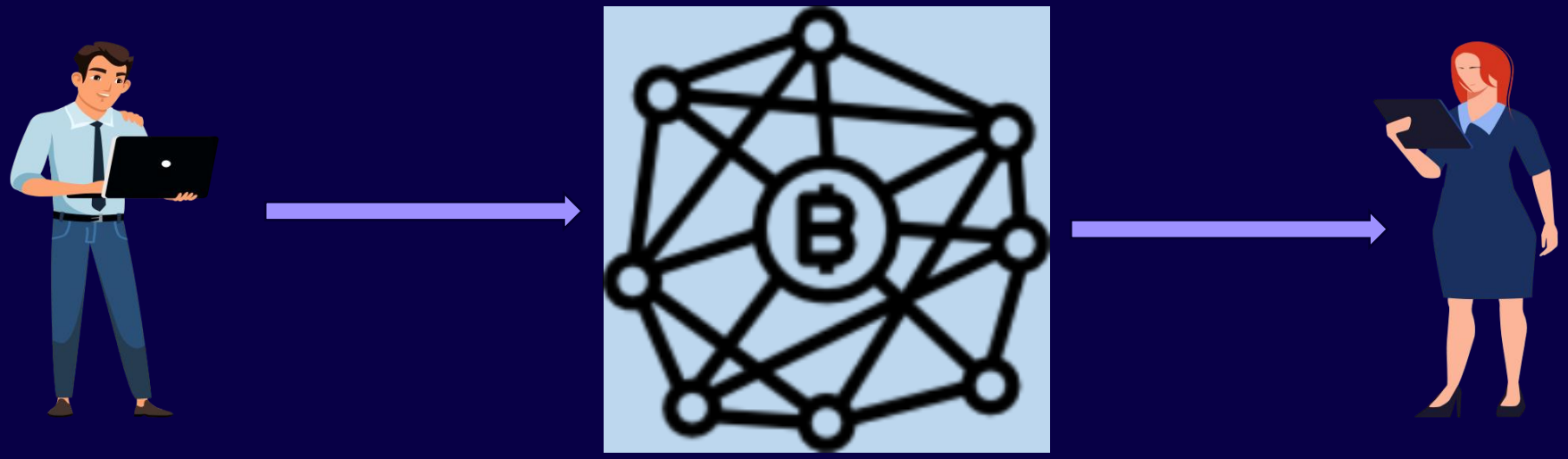
Stable Coins

1. Excessive volatility is a major flaw with many cryptocurrencies. This creates a barrier for customers who want to utilize DeFi apps but don't have the risk tolerance for a volatile asset like ETH.
   Stablecoins, a new type of cryptocurrency, have arisen to address this issue.
2. Stablecoins are designed to maintain price parity with a specific asset, such as the US dollar or gold.
3. Tether (USDT) is the largest fiat-collateralized stablecoin, with a market capitalization of $24 billion dollars, ranking third after Bitcoin and Ethereum.
4. Crypto-collateralized stablecoins are the second most common type of stablecoin.
5. DAI, founded by MakerDAO, is the most popular crypto-collateralized stablecoin

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Transactions

- The atoms of DeFi are Ethereum transactions.
- Data and/or ETH (or other tokens) are sent from one address to another in transactions.
- A transaction is the starting point for all Ethereum interactions.



Fungible Tokens

- Both conventional currency and cryptocurrencies are "fungible,"
- The fungibility of cryptocurrencies gives them a reliable method for carrying out blockchain transactions.
- Actually, assets or tokens that can be divided into multiples are fungible.

For instance,
Fungible fiat currencies include the dollar: A $1 bill is worth the same in Miami as it is in New York City. A cryptocurrency like Bitcoin can also be a fungible token: No matter where it is issued, one bitcoin is worth one bitcoin.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Fungible Tokens

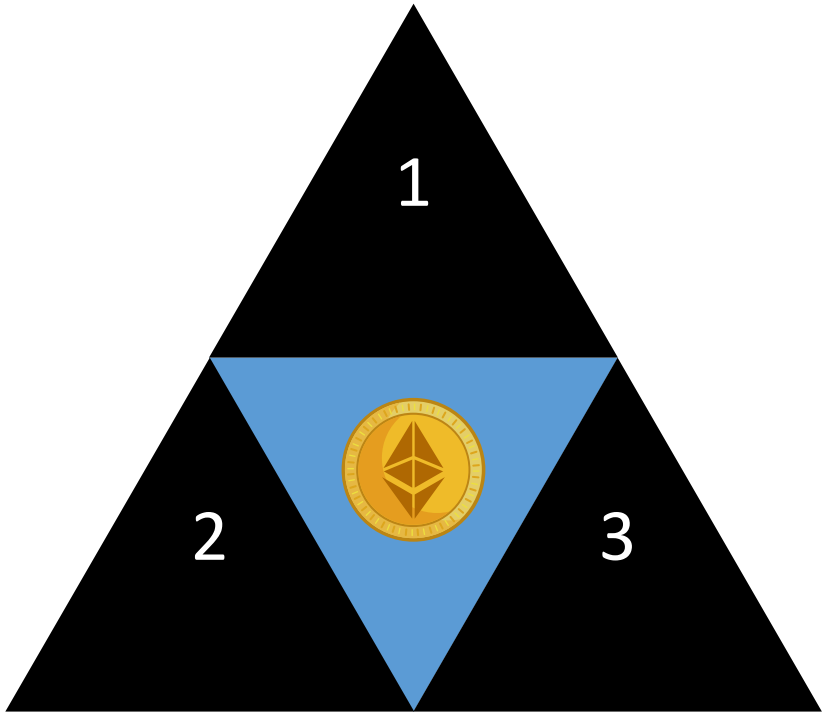
Utility Tokens

A utility token is a crypto token that serves a specific use case inside an ecosystem.

These tokens enable users to carry out a certain action on a network. A utility token is distinct within its ecosystem.

For example, Brave's Basic Attention Token (BAT) may only be used to tip content producers via the Brave browser or other programs that have integrated BAT wallets, such as Twitter.

What Are Utility Tokens Used For?

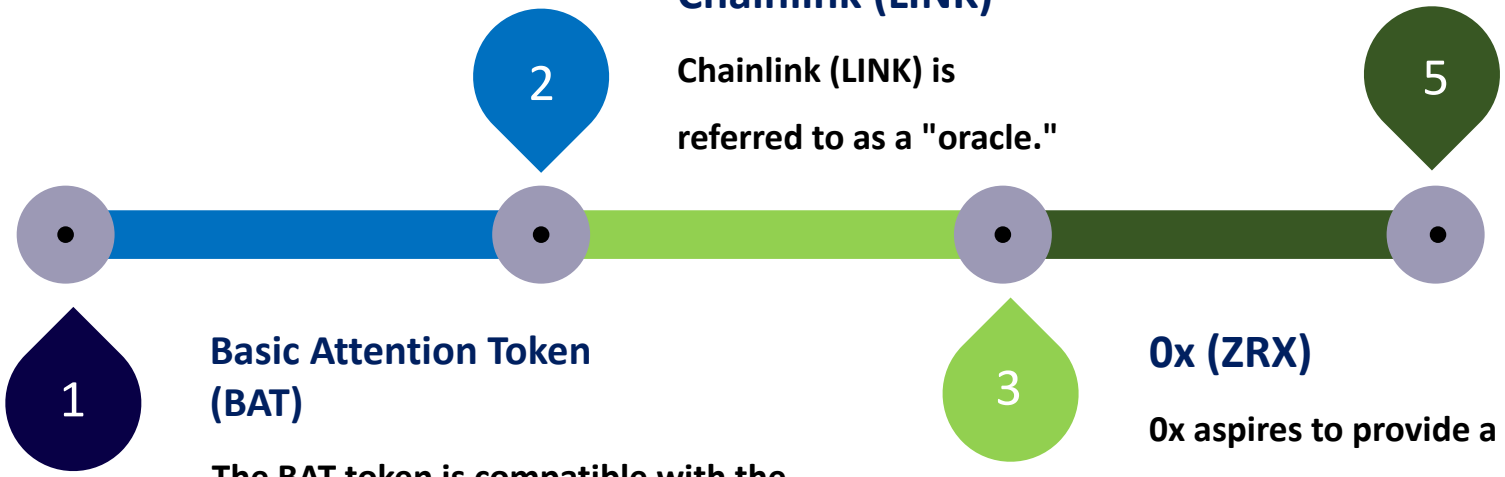


A utility token may be used for almost any purpose that a developer desires.

While cryptocurrencies are a type of digital money, utility tokens are more accurately defined as software.

A token of this type might be used to reward platform users or to pay interest to individuals who deposit cash that the platform subsequently loans out to borrowers.

Examples of Utility tokens



Basic Attention Token (BAT)

The BAT token is compatible with the Brave browser, which is intended to be safe and private.

Chainlink (LINK)

Chainlink (LINK) is referred to as a "oracle."

0x (ZRX)

0x aspires to provide a safe and quick crypto trading platform that combines characteristics of both centralized and decentralized exchanges.

Binance Coin (BNB)

Binance Coin (BNB) is a "exchange token," or a token that is native to the ecosystem of a certain crypto exchange.

Equity Token

An equity token is a token that reflects ownership of an underlying asset or pool of assets.

1

2

The units must be fungible, which means they must all correspond to the same share of the pool.

The pools of assets in true equity tokens can have considerably more sophisticated mechanisms than a static pool or predetermined rates of increase.

3

4

Only what can be encoded into a smart contract limits the possibilities.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

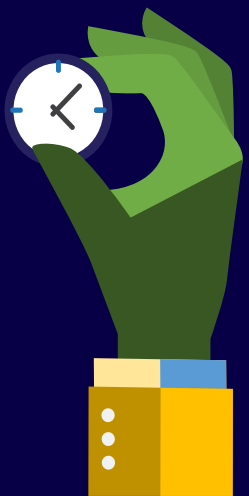
Government Token

1. Government tokens represent percentage ownership like equity tokens.
   The Owners of tokens enjoy voting rights.

2. The owners have the authority to alter the project's protocol or cast ballots to determine network rules.

3. Reasons for revealing these new forms of ownership are based on the accelerating pace of technological advancement and rising hazards. Decentralized autonomous organization (DAO) is one of these models.

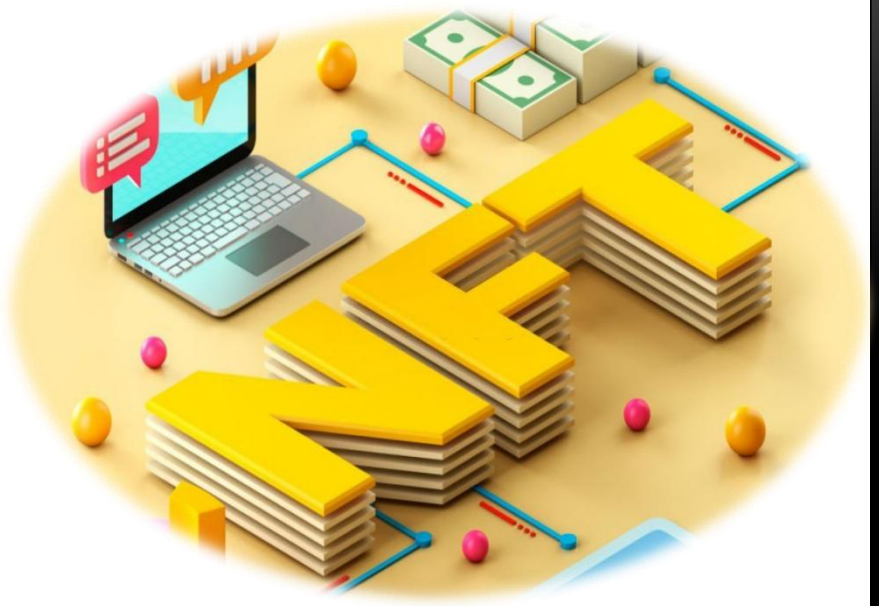
4. Here, the holders of the tokens gain authority in proportion to the magnitude of the stake.



TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

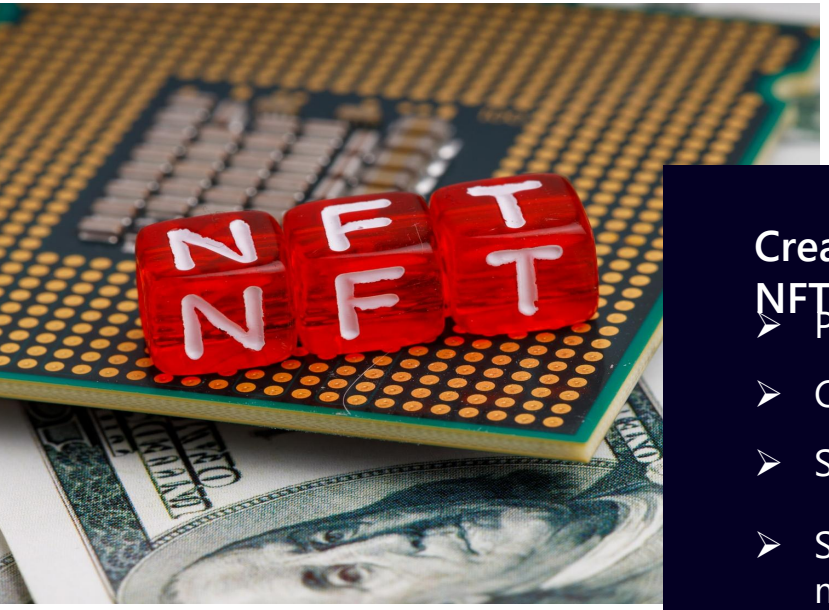
What Is a Non-Fungible Token (NFT)?

Non-fungible tokens (NFTs) are cryptographic assets on a blockchain that are different from each other because they have unique identification codes and metadata. They can't be traded or exchanged at the same value as cryptocurrencies.



- NFTs are unique cryptographic tokens that exist on a blockchain and cannot be replicated.
- NFTs can represent real-world items like artwork and real estate.
- "Tokenizing" these real-world tangible assets makes buying, selling, and trading them more efficient while reducing the probability of fraud.
- NFTs can also function to represent individuals' identities, property rights, and more.

Create, Buy, and Sell NFTs



Creating NFTs

- Pick your item
- Choose your blockchain
- Set up your digital wallet
- Select your NFT marketplace & upload file

Ways to Buy NFTs

- Purchase Ethereum
- Connect your MetaMask to an NFT Marketplace like OpenSea.
- Buy Your NFT

Ways to Sell NFTs

- Create an NFT based on a marketplace you've chosen
- List your NFT for sale
- Manage your listing

Lending- A Key Features (DeFi)

- The account holders can lend and borrow digital assets like in the real world.
- Institutional features mostly encourage speculating in digital assets rather than lending to the real economy
- DeFi financing is plagued with over-collateralization due to the presence of volatility.
- If a borrower's collateralization ratio falls below a certain level, their position is liquidated to pay off their loan.

Aave, A Loan Market Protocol

Aave, a decentralized financial protocol, enables the lending and borrowing of digital currency. The deposit of digital assets by lenders yields interest.

- Aave offers a large number of additional tokens to supply and borrow.
- The Aave loan and variable borrowing rates are more predictable
- Each market has its own set of token pools.
- The market's supported tokens can only be used in that certain market

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Derivatives- A Key Features (DeFi)

A derivative is a contract between two or more parties, the value of which is based on a predetermined underlying financial asset, such as a security or a group of assets.

Yield Protocol

1. **Yield Protocol presents a derivative model for zero-coupon bonds that are secured.**
   A yToken is an ERC-20 (fungible) token that settles in a defined quantity of a target asset at a given date.

2. **The tokens are backed by the collateral asset and have a needed maintenance collateralization ratio, similar to MakerDAO.**

3. **If the value of the collateral falls below the required level of maintenance, the position can be liquidated by selling some or all of the collateral to cover the obligation.**

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Derivatives- A Key Features (DeFi)

Synthetix

1. Synthetix is working on a brand-new derivative. It is a company whose main goal is to develop a wide range of liquid synthetic derivatives.

2. The company issues Synths, which are backed by collateral and whose prices are tied to an underlying price feed. DAI, MakerDAO's synthetic asset, is likewise a synthetic asset.

3. Synths may theoretically track any asset, including long and short, as well as leveraged positions.

Tokenization- A Key Features (DeFi)

Tokenization is the process of taking an asset or a group of assets, either on or off the blockchain, and either

- reflecting that asset on the blockchain with fractional ownership, or
- producing a composite token that holds a number of underlying tokens.

Now, the Benefits of Tokenization

1. **More Liquidity:** Boosts market liquidity and eliminates the "liquidity premium"

2. **Faster, Cheaper Transactions:** Plays role in significantly lowering transaction costs and processing times for each trade by passing market intermediaries and other middlemen.

3. **Transparency and Provability:** The immutability and transparency provided by blockchain technology assist ensure the veracity of each token's claimed history

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Risks associated with Decentralized Finance

Smart-Contract Risk

- Crypto-focused products have been regularly hacked over the last decade.
- Software is particularly vulnerable to hacks and developer errors.

Governance Risk

- Many additional protocols rely on humans to actively manage protocol risk and many of them utilize similar approaches which create governance risk.
- An enemy can simply buy a majority of the liquid governance tokens to take control of the protocol.

TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Risks associated with Decentralized Finance

Oracle Risk

- Oracles are one of the final unsolved challenges
- Blockchains without oracles are totally self-contained, with no awareness of the outside world

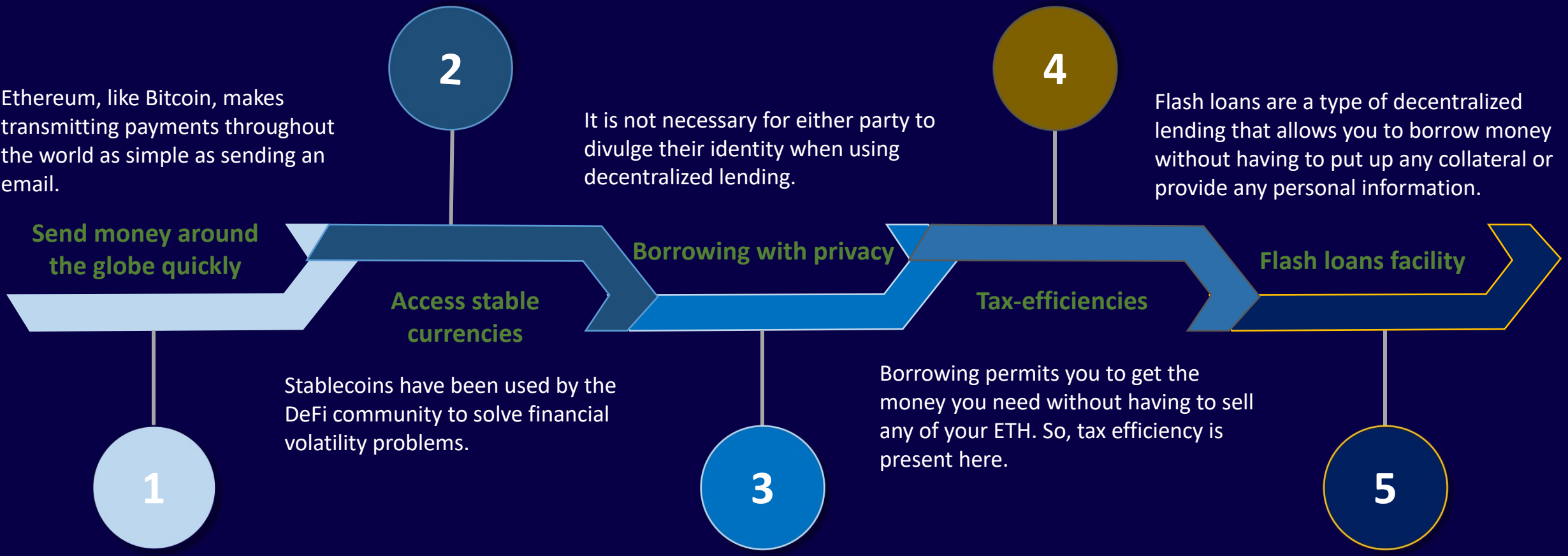
Scaling Risk

- DeFi is at risk of not being able to meet demand due to Ethereum's lack of scalability.
- New systems such as Polkadot, Zilliqa, and Algorand, on the other hand, offer some solutions to this scaling issue.

Regulatory Risk

- when we consider regulatory risk, we also consider the terms Know Your Customer (KYC) and Anti-Money Laundering (AML). When
- Several decentralized derivatives exchanges, such as dYdX, have already had to geoblock US consumers from using certain exchange features.

Features of Decentralized Finance



TECH COMMMANDERS
ADVANCING YOUR IT SKILLS

Advantages of Decentralized Finance

Programmability

Smart contracts with a high level of programmability automate execution and allow the creation of new financial instruments and digital assets.

Immutability

Data coordination across a blockchain's decentralized architecture is tamper-proof, which improves security and audibility.

Touching

Developers and product teams can construct interfaces and integrate third-party applications with DeFi by building on top of existing protocols.

Transparency

Every transaction on the public Ethereum blockchain is broadcast to the Ethereum network and confirmed by other users. So, transparency is assured here.

Permission less

DeFi, in contrast to traditional finance, is distinguished by its open, permission-less access.

Self-Custody

DeFi market participants always preserve custody of their assets and control of their personal data

Scopes of Decentralized Finance

Know Your Transaction (KYT)

Ethereum's decentralized infrastructure allows for next-generation compliance analysis based on the behavior of participating addresses rather than participant identities in the DeFi space.

DAOs

A Decentralized Autonomous Organization (DAO) is a decentralized autonomous organization that cooperates according to transparent rules inscribed on the Ethereum blockchain, removing the need for a centralized administrative agency.

Data and analytics

DeFi Pulse is one of many tools and dashboards that enable customers to track the value locked in DeFi protocols, measure platform risk, and compare yield and liquidity.

Scopes of Decentralized Finance

Insurance

Ethereum's decentralized infrastructure allows for next-generation compliance analysis based on the behavior of participating addresses rather than participant identities in the DeFi space.

DAOs

Here, Customers can now choose from a choice of new insurance options to help them get coverage and preserve their investments.

Payments

Users can exchange cryptocurrencies securely and directly with one another using blockchain technology, which eliminates the need for middlemen.

Thank You

I wish you much success on the exam and in your life!

Please reach out if I can be of assistance.

TECH COMMANDERS
ADVANCING YOUR IT SKILLS

- Contact me on LinkedIn
- Contact me on YouTube
- Contact me on Twitter
- Contact me on Steemit
- Contact me at Techcommanders

EMAIL
techie@techcommanders.com

WEBSITE
www.techcommanders.com

PHONE
(904) 512 5529