DeFi

- DeFi is an open and global financial system
- One of the blockchain’s strongest innovations is the transfer and trade of financial assets without trusted intermediaries.
- Decentralized Finance (DeFi), a new sub-field of blockchain, specializes in advancing financial technologies and services on top of smart contract enabled ledgers

  Decentralized Finance (DeFi) leverages the power of blockchain technology, particularly smart contracts, to create a new financial ecosystem.

Problems that exist today

- **Some people aren't granted access to set up a bank account or use financial services.**
- **Lack of access to financial services can prevent people from being employable.** your personal data is often considered a hidden charge. While you might not be explicitly billed for sharing your information, it comes at a cost in several ways
- **A hidden charge of financial services is your personal data.**
- **Governments and centralized institutions can close down markets at will.**
- **Trading hours are often limited to business hours of specific time zone.**
- **Money transfers can take days due to internal human processes.**
- **There's a premium to financial services because intermediary institutions need their cut.** intermediary institutions like banks and financial advisors charge fees for their service

three key segments of the banking system:

1. Payment & clearance system (remittance)

2. Accessibility

3. Centralization & Transparency

1. Payment Systems & Remittance:

Foundation of financial transactions: This encompasses the infrastructure for transferring funds between individuals, businesses, and across borders. It includes payment networks (e.g., credit cards, wire transfers), clearing systems, and the technology that facilitates seamless, secure transactions.
Key Impact: This is vital for the flow of money within an economy and for international trade, affecting everything from everyday purchases to large-scale investments.
2. Financial Accessibility:

Enabling inclusion: Accessibility focuses on how easy it is for individuals and businesses to access a wide range of financial services. This includes the availability of bank branches, ATMs, digital banking options, and financial products that meet diverse needs.
Key Impact: Financial accessibility is crucial for empowering individuals, fostering economic growth, and promoting financial stability. When people have access to savings accounts, loans, and insurance, it can improve opportunities for financial well-being and participation in the broader economy.

DeFi

- DeFi is an ecosystem of Decentralized Applications (Dapps) that provide financial services built on top of distributed networks with no governing authority.
- DeFi is a collective term for financial products and services that are accessible to anyone who can use Ethereum – anyone with an internet connection.
- no centralized authorities
- automatic and safer now that they're handled by code that anyone can inspect and scrutinize.

Limited scope: While smart contracts automate specific functions within DeFi applications, they cannot entirely replace the human element in financial services, which is crucial for tasks like risk assessment, fraud prevention, and customer support.
Code vulnerabilities: Even if the code is open-source and publicly available, vulnerabilities can still exist. Exploiting these vulnerabilities can lead to significant financial losses for users, as seen in several high-profile DeFi hacks.

The adoption curve for decentralised finance

- new approach to blockchain-powered finance
- locked-up assets grow from less than $1 billion in 2019 to the entire cryptocurrency market was valued at approximately $200 billion on the 31st of December 2019
- just two years later, attracting at least one million investors in the process.
- market that's expected to grow to $800 billion in 2022.

Infrastructure

. Blockchain: The underlying technology that powers DeFi. It acts as a distributed ledger, where transactions are recorded publicly, transparently, and immutably across a network of computers. This creates trust and security in the system without relying on a central authority.

2. Cryptocurrency: Digital assets built on top of blockchains. In DeFi, they serve as the primary medium of exchange and value storage for financial applications. Examples include Bitcoin and Ethereum.

3. The Smart Contract Platform/Decentralized Applications (DApps): These are essentially software programs built on top of blockchains, using smart contracts. Smart contracts are self-executing contracts stored on the blockchain that automatically execute pre-determined terms and conditions when specific conditions are met. DApps leverage smart contracts to offer various financial services like lending, borrowing, and trading.

- BLOCKCHAIN
- CRYPTOCURRENCY
- THE SMART CONTRACT PLATFORM/DECENTRALIZED APPLICATIONS
- STABLECOINS
- ORACLES

4. Stablecoins: Cryptocurrencies designed to maintain a stable value, often pegged to traditional assets like the US dollar (Most stablecoins maintain a 1:1 peg with a fiat currency like the US dollar. This means one stablecoin represents the equivalent of one US dollar). This helps mitigate the high volatility often associated with other cryptocurrencies, making them more suitable for financial transactions within DeFi.

Oracles: Bridge the gap between blockchain networks (offline) and the real world (online). They fetch and deliver external data to smart contracts, allowing them to react to and interact with real-world events. This is crucial, as smart contracts rely on accurate data to function properly.

Blockchain: Provides the secure and transparent foundation.
Cryptocurrency: Acts as the medium of exchange and value storage.
Smart Contract Platforms/DApps: Build the applications that offer financial services.
Stablecoins: Offer stability for financial transactions.
Oracles: Connect DeFi to the real world for broader functionality.

Key Components of DeFi

To create a financial ecosystem capable of bypassing banks, brokers, exchanges and the other middlemen who traditionally manage and process financial services.

- **digital assets**
- **Wallets**
- **smart contracts and**
- **auxiliary services including oracles**

1. Digital Assets:

Foundation of Value: These are the digital tokens or coins used within the DeFi ecosystem. They can represent various things, including currencies, stocks, bonds, and even real-world assets like property. Examples include Bitcoin, Ethereum, and various DeFi-specific tokens.
2. Wallets:

Secure Storage and Access: These are digital or physical tools that allow users to store, manage, and transfer their digital assets. They come in various forms, such as software wallets, hardware wallets, and mobile wallets. Users need secure wallets to interact with DeFi applications and manage their holdings.
3. Smart Contracts:

Automated Execution: These are self-executing contracts written in code and stored on the blockchain. They define the terms of an agreement and automatically execute when pre-specified conditions are met. Smart contracts enable trustless transactions and automate various DeFi functions like lending, borrowing, and trading.
4. Auxiliary Services (including Oracles):

Expanding Functionality: These components provide additional functionalities that support the DeFi ecosystem. Oracles, for example, act as bridges between the blockchain and the real world. They fetch and deliver external data to smart contracts, allowing them to react to and interact with real-world events.
Other examples: Include decentralized exchanges (DEXs) for peer-to-peer trading, decentralized asset management platforms, and lending/borrowing protocols.

to grow vigorously

What is it about Ethereum that allows decentralized finance applications to thrive?

- Open access
- Stablecoins
- A new token economy
- Interconnected financial services

Open Access:
Permissionless Network: Unlike traditional financial systems with restricted access, Ethereum operates as a permissionless network. This means anyone can join the network, participate in DeFi activities, and develop their own applications without seeking approval from a central authority. This fosters innovation and empowers users to take control of their financial activities.

Other Contributing Factors:

Stablecoins: The emergence of stablecoins like Tether (USDT) and USD Coin (USDC) built on Ethereum provided a crucial element of stability and facilitated wider adoption of DeFi applications.

Token Economy: Ethereum's native token, Ether (ETH), plays a vital role. It's used for gas fees (transaction costs) within the network, incentivizes participation in network security, and can be used as collateral or a medium of exchange within DeFi applications.

Interconnected Financial Services: The Ethereum ecosystem boasts a diverse range of interconnected DeFi applications, including decentralized exchanges (DEXs), lending/borrowing protocols, and yield farming opportunities. This interconnectedness allows users to seamlessly switch between different DeFi services to optimize their financial activities.

Common services offered by DeFi platforms

- Payments
- Loans
- Trades
- Investments
- insurance and
- asset management
- liquidity mining
- Send money around the globe
- Stream money around the globe
- Access stable currencies
- Borrow funds with collateral
- Borrow without collateral
- Start crypto savings
- Trade tokens
- Grow your portfolio
- Fund your ideas
- Buy insurance
- Manage your portfolio

Liquidity mining is a way for people to earn rewards by providing liquidity to decentralized finance (DeFi) protocols. In DeFi, liquidity refers to the availability of assets (like cryptocurrencies) for trading.

The list is growing rapidly and provides a tantalising glimpse of a new era of crypto-based innovations, such as decentralised exchanges, synthetic assets and flash loans.

The benefits of DeFi

- **DeFi is permissionless and inclusive**
- **Transactions are in real time/speed**.
- Accessible to all.
- **Transactions are transparent, immutable and tamper proof**
- **Users can retain custody of their assets** users hold control of their own cryptocurrencies and other digital assets
- **Smart contracts are highly programmable**
- **DeFi data is tamper proof, secure and auditable**
- **Many DeFi protocols are open source.**
- enhanced security
- cost-efficiency.

Collateral is money or property which is used as a guarantee that someone will repay a loan.

The risks of DeFi

- DeFi technology is immature
- A lack of consumer protection.
- Hackers are a threat (transparent).
- Collateral requirements are high.
- Private key requirements.
- Scalability: In most cases, the bandwidth of a DeFi is limited to the blockchain it resides on.

Lack of Consumer Protection:

Absence of central authority: Unlike traditional finance with regulatory bodies and established consumer protection frameworks, DeFi operates in a decentralized environment. This means there's no central authority or regulatory body to oversee the activities of DeFi applications and protocols. This lack of oversight can leave users vulnerable to various risks:

Scams and fraudulent activities: Malicious actors can create fake DeFi projects or exploit vulnerabilities in existing ones to steal user funds.

Misleading information and marketing: Without centralized oversight, users may encounter misleading information or aggressive marketing tactics that could lead them to make risky investment decisions.

Unresolved disputes: In case of disputes or issues with a DeFi application, there are often no established mechanisms for users to seek recourse or compensation, unlike traditional financial

DeFi's scalability being limited to the underlying blockcha

Collateralization in DeFi:

Loan Security: Unlike traditional lenders who rely on credit scores and other financial history, DeFi lending protocols require users to deposit collateral, which is an asset they own, to secure a loan. This collateral acts as a guarantee for the lender. If the borrower defaults on the loan (fails to repay), the lender can then seize the collateral to recoup their losses.
High Requirements: The amount of collateral required is often significantly higher than the value of the loan itself. This loan-to-value (LTV) ratio can range from 150% to 300%, meaning you need to deposit 1.5x to 3x the value of the loan as collateral.

Custodial and Non custodial Wallets

Non custodial Wallets

- Argent(Mobile Phones)
- Metamask(PC/Laptops)

Custodial wallets:

Easier to use: Good for beginners.
Less control: Third-party holds your keys, like a bank.
Recovery options: May help if you lose login information.
Non-custodial wallets:

More control: You hold the keys, like cash in your pocket.
More complex: Requires technical knowledge and personal security responsibility.

Metamask acts as both a wallet and an interaction bridge for the Ethereum network.

entire Ethereum blockchain of over 400GB downloaded on your computer

Argent (Mobile Phones): This mobile-only wallet prioritizes user-friendliness and offers features like social recovery and multi-signature security. It's a good option for individuals starting with cryptocurrency and seeking a convenient mobile solution.
Metamask (PC/Laptops): This browser extension wallet provides access to a wider range of DeFi applications and features compared to Argent. However, it comes with the trade-off of requiring users to download the entire Ethereum blockchain (currently over 400GB) to their computer for full functionality.

Wallets

https://ethereum.org/wallets/find-wallet

- **New to crypto:** Torus Wallet, Coinbase Wallet
- **NFTs:** Taho, Coinbase Wallet
- **Hodler:** Ledger, OneKey
- **Finance:** Ledger, Coinbase Wallet,Taho

For Newcomers to Crypto:

Torus Wallet: This mobile wallet uses facial recognition or fingerprint authentication for login, offering a user-friendly experience for beginners.
Coinbase Wallet: This custodial wallet provides a simple interface and is integrated with the popular Coinbase exchange, making it convenient for beginners to buy and store cryptocurrency.
For NFT (Non-Fungible Token) Storage:

Taho: This mobile and browser wallet focuses on security and user experience for managing NFTs.
Coinbase Wallet: While not strictly an NFT-specific wallet, Coinbase Wallet allows storing and viewing NFTs alongside other cryptocurrencies.
For Hodlers (Long-Term Investors):

Ledger: These hardware wallets offer a secure, offline storage solution for cryptocurrencies, ideal for hodlers who prioritize long-term security.
OneKey: Another hardware wallet option with similar features to Ledger, providing offline storage and security for hodlers.
For DeFi (Decentralized Finance) and Financial Activities:

Ledger: Hardware wallets like Ledger can be used to interact with DeFi applications and protocols securely, allowing users to participate in various financial activities.
Coinbase Wallet: While primarily a custodial wallet, Coinbase Wallet integrates with some DeFi applications, allowing users to explore basic DeFi functionalities.
Taho: Again, while not strictly a DeFi wallet, Taho allows connecting to certain DeFi applications for limited financial activities.

Comparison between **DeFi vs traditional finance**

Pseudonymity: Activities are linked to an identifier, but not your real-world identity. Think of it like using a screen name on the internet – you're trackable by the screen name, but your true identity remains hidden.

DeFi

- You hold your money.
- You control where your money goes and how it's spent.
- Transfers of funds happen in minutes.
- Transaction activity is pseudonymous.
- DeFi is open to anyone.
- The markets are always open.
- It's built on transparency – anyone can look at a product's data and inspect how the system works.

Traditional Finance

- Your money is held by companies.
- You have to trust companies not to mismanage your money, like lending to risky borrowers.
- Payments can take days due to manual processes.
- Financial activity is tightly coupled with your identity.
- You must apply to use financial services.
- Markets close because employees need breaks.
- Financial institutions are closed books: you can't ask to see their loan history, a record of their managed assets, and so on.

Important Terms

- Financial Institutions refer to financial intermediaries.
- Financial Instruments refer to monetary assets.
- Financial Markets refer broadly to any marketplace.

Financial Institutions:

Definition: Organizations that act as intermediaries between individuals, businesses, and governments in financial transactions. They provide various financial services like:
Savings and loans: Accepting deposits and offering loans.
Investments: Facilitating buying and selling securities.
Payments: Processing payments and money transfers.
Insurance: Providing financial protection against risks.
Examples: Banks, credit unions, insurance companies, brokerage firms, investment banks.

Financial Instruments:

Definition: Assets that represent a financial claim or obligation. They hold monetary value and can be traded or exchanged. They are essentially tools used to store, transfer, or invest funds.
Examples:
Stocks: Ownership shares in a company.
Bonds: IOUs issued by governments or corporations, offering a fixed interest rate and repayment schedule.
Derivatives: Contracts derived from the value of underlying assets (e.g., options, futures).
Deposits: Funds placed in a financial institution for safekeeping and potential interest earnings.
Loans: Borrowed funds with an obligation to repay with interest.

Financial Markets:

Definition: Platforms where buyers and sellers come together to trade financial instruments like stocks, bonds, and currencies. They facilitate the flow of funds between borrowers and investors.
Examples:
Stock market: Where stocks of publicly traded companies are bought and sold.
Bond market: Where bonds issued by governments and corporations are traded.
Foreign exchange market (Forex): Where currencies are traded.
Derivatives markets: Where derivative contracts are traded.

Distinctive features

1. **Transparency**. In DeFi, a user can inspect the precise rules by which financial assets and products operate. DeFi attempts to avoid private agreements, back-deals and centralization, which are significant limiting factors of CeFi transparency.

2. **Control.** DeFi offers control to its users by enabling the user to remain the custodian of its assets, i.e., no-one should be able to censor, move or destroy the users' assets, without the users' consent.

3. **Accessibility.** Anyone with a moderate computer, internet connection and know-how can create and deploy DeFi products, while the blockchain and its distributed network of miners then proceed to effectively operate the DeFi application. Moreover, the financial gain in DeFi also presents a significant contrast to CeFi.

- In the years 2020 and 2021, DeFi offered higher annual percentage yields (APY) than CeFi: the typical yield of USD in a CeFi bank is about 0.01% , while at the time of writing, DeFi offers consistent rates beyond 8%.

Properties of DeFi

- Public Verifiability
- Custody
- Privacy
- Atomicity
- Execution Order Malleability
- Transaction Costs
- Non-stop Market Hours
- Anonymous Development and Deployment

Public Verifiability: Transactions and smart contracts on a blockchain are publicly accessible and independently verifiable by anyone, ensuring transparency and trust.
Custody: In true DeFi applications, users maintain custody of their assets through non-custodial wallets, giving them complete control.
Privacy: While transactions are publicly viewable, they are often pseudonymous, protecting users' real-world identities to some degree (privacy coins enhance this further).
Atomicity: DeFi transactions often occur atomically, meaning they either succeed completely or fail completely. This prevents partial transactions and ensures consistency in the system.
Non-stop Market Hours: Decentralized exchanges and other DeFi applications run 24/7, unlike traditional financial markets that have operating hours.
Additional Considerations:

Execution Order Malleability: This refers to the potential for transactions to be reordered within a block on the blockchain. This can lead to issues like front-running, where someone can observe a pending transaction and place their own trade ahead of it.
Transaction Costs: These refer to the fees associated with transacting on a blockchain network, commonly referred to as "gas fees." Fees can fluctuate depending on the network congestion and the complexity of the transaction.
Anonymous Development and Deployment: Some DeFi projects are initiated by anonymous individuals or teams, adding a layer of mystery and potential lack of accountability compared to traditional financial systems.

The decision tree helps categorize different financial protocols as either DeFi (Decentralized Finance) or CeFi (Centralized Finance) based on three key criteria:

Control of Assets: Whether users have complete control of their financial assets without relying on a third-party custodian. (Do they use non-custodial wallets?)
Censorship of Transactions: Whether a single entity has the power to prevent or block a transaction.
Censorship of the Protocol: Whether a single entity has the power to prevent protocol execution or alter its rules.

How the Tree Works:

Are the financial assets controlled by the user (non-custodial)?

Yes: The protocol is on the path toward DeFi.
No: We move to the next question.
Can someone single-handedly censor a transaction execution?

Yes: We move to the next question.
No: The protocol is leaning towards DeFi.
Can someone single-handedly censor the protocol execution?

Yes: The protocol is classified as CeFi Intermediary, DeFi Settlement (explained later).
No: The protocol is classified as fully DeFi.

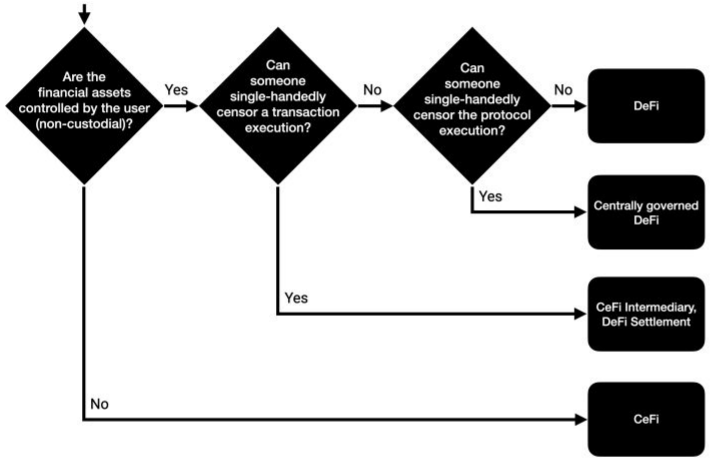


Figure 1: Decision tree to differentiate among DeFi and CeFi.

Explanation of Categories:

DeFi: A fully decentralized financial system where users have full control over their assets, and no single entity can censor transactions or protocol execution.
CeFi: A centralized financial system where a company or intermediary controls user assets and manages transactions.
CeFi Intermediary, DeFi Settlement: A hybrid model where trading may occur in a decentralized manner, but the final settlement and custody of assets are still controlled by a centralized entity.

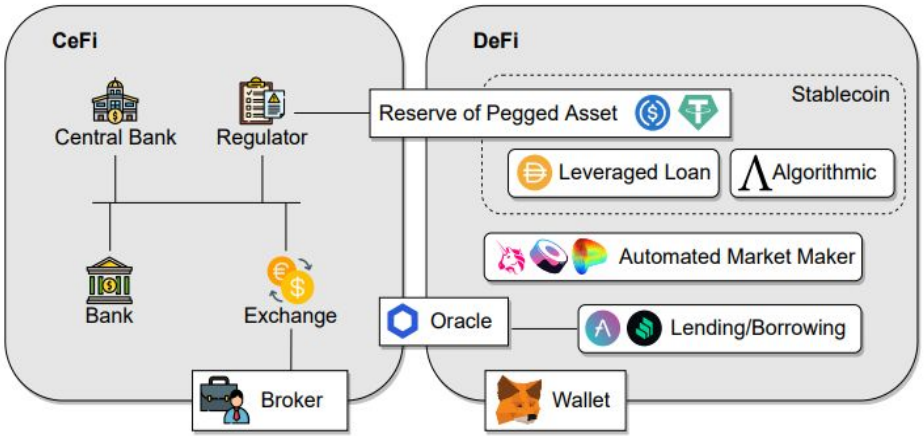


Figure 3: High-level service architecture of CeFi and DeFi.

CeFi vs. DeFi Exchanges

Nine elements of DeFi are discussed:

1. Token transfers: native blockchain transactions
2. Market making via smart contracts:Market makers provide liquidity in cryptocurrency markets
3. Oracles: importing external data
4. Borrow/Lending: banking functionality
5. Cross border finance: bridges, wrapped tokens
6. Stable coins: tying tokens to fiat
7. Synthetics: self-adapting financial instruments
8. NFTs : digital collectibles
9. DAOs : tokenized governance

Terra UST

Terraform DO Kwon danieal shill

Terra blockchain project 2018

UST pegged usd

Luna pegged KRW

Burn 1 luna worth of 1usd of tokens to mint 1ust

 Burn 1ust tokens to mint 1usd worth of luna

ust>1usd, sell ust by burning luna

ust<iusd

DeFi Key Categories

1. Stablecoins
2. Exchanges
3. Lending and Borrowing
4. Derivatives
5. Fund Management
6. Lottery
7. Payments
8. Insurance

1. Stablecoins

Tether USDT, USDC,DAI,UST,LUNA

ASSET: Tether USDT

FIAT:USDC

CRYPTO: DAI

ALGORITHMS:UST,LUNA

Function: Cryptocurrencies designed to maintain a stable price, typically pegged to a fiat currency (like USD) or a basket of assets.
Benefits: Reduce the price volatility often associated with other cryptocurrencies, making them suitable for transactions and storing value.
Examples: Tether (USDT), USD Coin (USDC), Dai (DAI)

2. Exchanges

- **Centralized exchange (CEX),** a digital marketplace where crypto trading takes place, Binance, Kraken, Coinbase
  - they are both the intermediaries and custodians of the assets being traded.
  - user-friendly and generally offer more liquidity and stronger regulatory assurances
  - central company running the exchange has a lot of power and responsibility for the financial stability and health of the exchange.
  - by a small handful of professional trading firms with permissioned access and specialized tools

- Decentralized exchange (DEX): Uniswap and Pancakeswap
  - Decentralized exchanges aim to solve this issue by allowing users to exchange cryptocurrencies without giving up custody of their coins.
  - lower transaction fees, let users directly hold their own assets and avoid some regulatory burdens

- In late 2021, the leading DEX Uniswap was charging a 0.05% transaction fee on the $100,000, CEXs Binance, Coinbase and Kraken were charging 0.1%, 0.2% and 0.2%, respectively.
- DEXs use “automated market maker” protocols to determine the prices of assets without a centralized body orchestrating trades.
  - If a certain pool contained very little ETH, it would have to let traders sell ETH into the pool at a higher price than the wider market indicated. Traders could easily profit by buying it in the wider market and selling it into the pool. As they did so, the volume in the pool would rise, reducing its offered price until it matched the wider market.

Impermanent loss: A big problem for DEXs

- Liquidity providers are entitled to withdraw the portion of the value of the pool they contributed, not the exact number of tokens they put in.
- This means that a liquidity provider will tend to end up withdrawing more of the tokens that lost value and less of the one that gained value, compared with their starting assets

Centralized Exchanges (CEXs)

Custodial Model: You're absolutely correct, CEXs act as custodians, holding users' assets on their behalf. This means users relinquish control of their private keys, essentially handing their funds over to the exchange.
Benefits: User-friendliness, higher liquidity (more buyers and sellers, making trades faster), and regulatory compliance are all strong benefits of CEXs.
Risks: The centralized nature of CEXs exposes them to potential hacks, mismanagement of funds, or regulatory shutdowns, all impacting users' assets.
Decentralized Exchanges (DEXs)

Non-custodial Nature: DEXs empower users with full custody of their assets. Users manage their private keys and interact directly with the exchange's smart contracts.
Benefits of the model: Increased security (users don't lose assets in case of exchange failure), more privacy, and potential resistance to censorship.
Challenges: Can be less user-friendly, and have lower liquidity than CEXs in some cases.
Transaction Fees

While you noted DEXs often having lower fees in the past, this dynamic can shift. Fees on CEXs and DEXs fluctuate based on market demand and network congestion. It's essential to check prevailing fees before making a trade.

Impermanent Loss

Key risk for DEX liquidity providers: When the price of assets in a liquidity pool diverges, the value of a liquidity provider's holdings can decrease compared to simply holding the assets outside the pool.
Not a guaranteed loss: The loss is 'impermanent' because it can be reversed if prices return to the levels they were at when assets were deposited.
Mitigating risk: Some DEXs have mechanisms to reduce impermanent loss or provide incentives that may offset losses.

3. Lending and Borrowing

- The global cryptocurrency market is projected to reach USD 4,067.4 million by 2027.
- one of the innovative financial services that is definitely gaining momentum is crypto lending and borrowing.
- allows crypto holders to leverage their digital assets for various purposes while offering opportunities for those seeking to borrow.
- 21% of American adults owned cryptocurrency as of 2022, crypto lending market has been growing substantially, with Compound's estimated market cap reaching $1.4 billion as of March 2022.
- This figures indicates there is a substantial increase in adoption and usage of cryptocurrency.

Function: Platforms enabling users to lend or borrow cryptocurrencies, earning interest on their holdings or accessing liquidity.
Benefits: Creates opportunities for passive income generation and borrowing without traditional credit checks.
Examples: Aave, Compound, MakerDAO

Crypto lending

- **Crypto lending platforms:** each with unique offering features and services.
  - **BlockFi :**Users can earn interest on their holdings, access loans, and participate in trading, all under one roof.
  - **Celsius Network:** not only facilitates lending and borrowing but also rewards its users
  - **Nexo:**offers crypto loans

Crypto Borrowing

- useful for leveraging investment opportunities or managing short-term financial needs.

4. lottery:Prolitus

global lottery industry is a **billion-dollar market** offered incredible money-making opportunities – to issuers and participants.

conventional lottery system is centralized, all aspects of lottery, such as issuance, purchase, draw, cashing, and the use of raised funds, lack visibility. Other inefficiencies plaguing the lottery industry include:

- Expensive Licensing Processes
- Inability To Offer Large Jackpots
- Hidden Costs
- High risk of fraud.
- Lack of Transparency
- Centralization and Control
- Limited Accessibility

Function: Decentralized platforms offering lottery games with potentially lower fees and higher transparency compared to traditional lotteries.
Benefits: Increased trust and verifiability through blockchain technology.
Examples: PoolTogether, PolyLotto

The core features of blockchain that has transformed the traditional lottery model

- Infallible
- Reliable
- Transparent/Zero Scope Of Confusion
- Democratic
- Eliminates Third Party Functions
- Easy Integration

The development of DeFi lottery platforms offers numerous advantages over traditional systems. Here are some key benefits:

1. Transparency and Trust

2. Enhanced Security

3. Global Reach and Inclusivity

4. Limitless Accessibility

Here are a few key aspects that demonstrate their potential impact:

1. Innovation and Evolution
2. Decentralization of Gambling
3. Cross-Chain Compatibility
4. Integration with Traditional Gambling

Function: Financial contracts derived from the value of underlying assets (e.g., cryptocurrencies, commodities) allowing for speculation, hedging, and leverage.
Benefits: Enables advanced trading strategies and risk management.
Examples: Synthetix, dYdX, Perpetual Protocol

5. Derivatives

Derivatives are contracts that derive their value from the underlying asset or group of assets. These are widely used to speculate and make money.

Asset: stocks, bonds, currencies, commodities and market indices.

The value of the underlying assets keeps changing according to market conditions.

The basic principle behind entering into derivative contracts is to earn profits by speculating on the value of the underlying asset in future.

Investors enter into derivative markets:

- Arbitrage advantage
- Protection against market volatility
- Park surplus funds

6. Fund Management

Fund management is the process of overseeing your assets and managing its cash flow to generate a return on your investments.

Function: Decentralized investment platforms allowing users to pool their funds and invest in a basket of cryptocurrencies or DeFi protocols, managed by automated algorithms or community governance.
Benefits: Provides access to diversified investment strategies and potentially higher returns.
Examples: yearn.finance, Compound Finance

Types:

- **Active fund management**
- **Passive fund management**

Active management requires frequent buying and selling in an effort to outperform a specific benchmark or index. Active management portfolios strive for superior returns but take greater risks and entail larger fees.

Passive management replicates a specific benchmark or index in order to match its performance.

Active funds generally have higher expense ratios due to the extensive research, analysis, and management activities performed by the fund manager. On the other hand, passive funds have lower expense ratios because the fund manager's role is limited, and the investment strategy is relatively straightforward.

An active investor is someone who buys stocks or other investments regularly. These investors search for and buy investments that are performing or that they believe will perform. If they hold stocks that are not living up to their standards, they sell them.

A passive investor rarely buys individual investments, preferring to hold an investment over a long period or purchase shares of a mutual or exchange-traded fund. These investors tend to rely on fund managers to ensure the investments held in the funds are performing and expect them to replace declining holdings.

- According to researchers, 1% corruption reduces 0.72% growth rate and 2% productivity of a country.
- making blockchain appropriate for funds collection processes by giving organizations, beneficiaries, donors, and legal authorities more control over the information and promoting data transparency. Hence, blockchain may be used to establish a safe money trail.
- In DeFi, fund management is conducted in a manner where it removes the investment manager and lets you choose the asset management strategy that best suits your financial need.
- The decentralized fund management also reduces the fees paid.

7. Insurance

- Insurance business runs on TRUST.
- but it has been breached by several times, due to which many insurance companies have paid the fraudulent claims, due to lack of evidences.
- Every year claims and underwriting fraud cost $80 billion and ~ $34 billion, specifically to Property and Casualty (P&C)Industry (per wnsdecisionpoint report).

Function: Decentralized protocols offering insurance products against smart contract vulnerabilities, hacks, and other DeFi-related risks.Benefit

Examples of DeFi platforms and services offered

(https://ethereum.org/en/dapps/?category=finance)

- **Lending and borrowing:** Aave, Oasis, compound etc
- **Exchanges:**Uniswap,Balancer, Curve
- **Demand aggregators:** KyberSwap, Matcha
- **Investment funds:** PoolTogether, Convex
- **Portfolio management:** Krystal, Rotki
- **Insurance:** Nexus Mutual
- **Payments:** Sablier
- **Crowdfunding:** Gitcoin Grants
- **Derivatives:** Synthetix
- **Liquid staking:**Lido
- **Prediction markets:** Augur

DeFi PRIMITIVES: DeFi primitives can be used as “building blocks” for larger financial assets.

- Mechanics
  - Transactions
  - Fungible Tokens
  - Non-fungible Tokens
- Supply and ownership
  - Custody
  - Supply Adjustment
  - Incentives
- Swap
- Loans
  - Collateralized Loans
  - Flash (Uncollateralized) Loans

Transactions

- Ethereum transactions are the atoms of DeFi.
- Transactions involve sending data or ETH (or other tokens) from one address to another

  two types of addresses: the *externally owned account* (EOA) and an address of a *contract account*.

  Bitcoin, all addresses are EOA.

pAYMENTS

Function: Emerging solutions aimed at facilitating fast, secure, and borderless payments using cryptocurrencies.
Benefits: Potential for lower transaction fees and wider accessibility compared to traditional payment methods.
Examples: The Graph, xDai

Transactions are signed messages recorded on blockchains.

need an entity called an account to do it for you.

The Ethereum blockchain keeps track of all the accounts and their balances in something called the state. Sending a transaction is the only way to trigger the change of state of an account.

There are two main types of accounts involved in transactions:

- ★ **Externally Owned Accounts (EOA).**
  - MOST COMMON TYPE OF ACCOUNT, controlled by private key, used for sending transactions, no associated code.
  - These are accounts controlled by private keys. The public key is the identifier of the account. An EOA account's public address is derived from its private key..Transactions are signed by the private key to prove ownership of the EOA. An EOA can be thought of as an individual's bank account that can be used to send funds using password verification.An EOA can only be controlled using its private key
- ★ **Contract Accounts.** These are accounts containing code and identified by a public key. A contract account has an associated code that executes when it receives a transaction from an EOA. A contract's public address is created by the combination of a public address of creating account + nonce. The code is commonly referred to as a smart contract and is an automated program that runs when it receives a transaction from another EOA or contract account.

Any transaction ultimately originates from an EOA. Contract accounts do not execute on their own.

Different ways that transactions can occur

Between EOAs directly

Between EOAs and Contract Accounts

Between Contract Accounts.

Atomicity

Clauses in a smart contract can cause a transaction to fail and thereby revert all previous steps of the transaction; as a result, transactions are *atomic*. Atomicity is a critical feature of transactions because funds can move between many con tracts (i.e., exchange hands) with the knowledge and security that if one of the conditions is not met, the contract terms reset as if the money never left the starting point.

complexity of the transaction: gas fee varies

Tokenization

- Tokenization is a Process of representing real-world assets as digital tokens on a blockchain
- Tokens can be stored, moved, and recorded on blockchain.
- Types of Assets: Real estate, stocks, commodities, art, intellectual property, etc.

Process of Tokenization

- Asset Identification: Selection of asset to be tokenized
- Legal Compliance: Compliance with regulations governing asset tokenization
- Token Design: Determining token characteristics (e.g., supply, divisibility)
- Smart Contract Development: Creating smart contracts to govern token issuance, transfer, and management

Security Requirement

Tokenization system should provide a proof of correct execution of transactions i.e, protection from double spending attacks.

Security Model

Each asset management requires two types of trust.

- Trust to a token issuer (proof of 1:1 ratio for collateral)
- Trust to a transaction processing system (protection from double spending attacks).

Advantages of Tokenization in Blockchain

- Fractional Ownership: Enables fractional ownership of high-value assets
- Accessibility: Allows global access to investment opportunities
- Liquidity: Facilitates trading and liquidity for traditionally illiquid assets
- Transparency: Transparent ownership records on the blockchain
- Security: Immutable and tamper-proof transactions
- Lower management cost
- Eliminate middle man
- Quick and cheaper transactions

Use Cases of Tokenization

- Real Estate: Fractional ownership of properties
- Art and Collectibles: Tokenizing ownership of artworks and collectibles as NFTs
- Securities: Issuance of digital securities representing ownership in companies
- Commodities: Tokenization of commodities such as gold, oil, etc.
- Intellectual Property: Representing ownership of patents, copyrights, etc.

Ex:Tokenization of real world assets

Assets	Tokenized by
gold and other commodities	DigiX, Platform for tokenizing physical assets such as gold and other commodities
gold	DigiX Gold (DGX),Tokenized gold backed by physical gold bullion
Real Estate	RealIT
Bonds	Society Generate
Equity	Spice VC
Paintings	Andy warhol

Tokenization Process

Acquisition of Physical Gold: Procurement and storage of gold bullion in secure vaults

Asset Verification: Independent audits and verification of gold reserves

Token Issuance: Creation of DGX tokens equivalent to the stored gold

Redemption: Ability to redeem DGX tokens for physical gold

Advantages of DigiX

Stability: Backed by physical gold, providing stability and hedge against market volatility

Accessibility: Enables fractional ownership of gold, making it accessible to a wider audience

Liquidity: Facilitates trading and liquidity through digital exchanges and platforms

Transparency: Transparent audit trail of gold reserves on the blockchain

Use Cases of DigiX

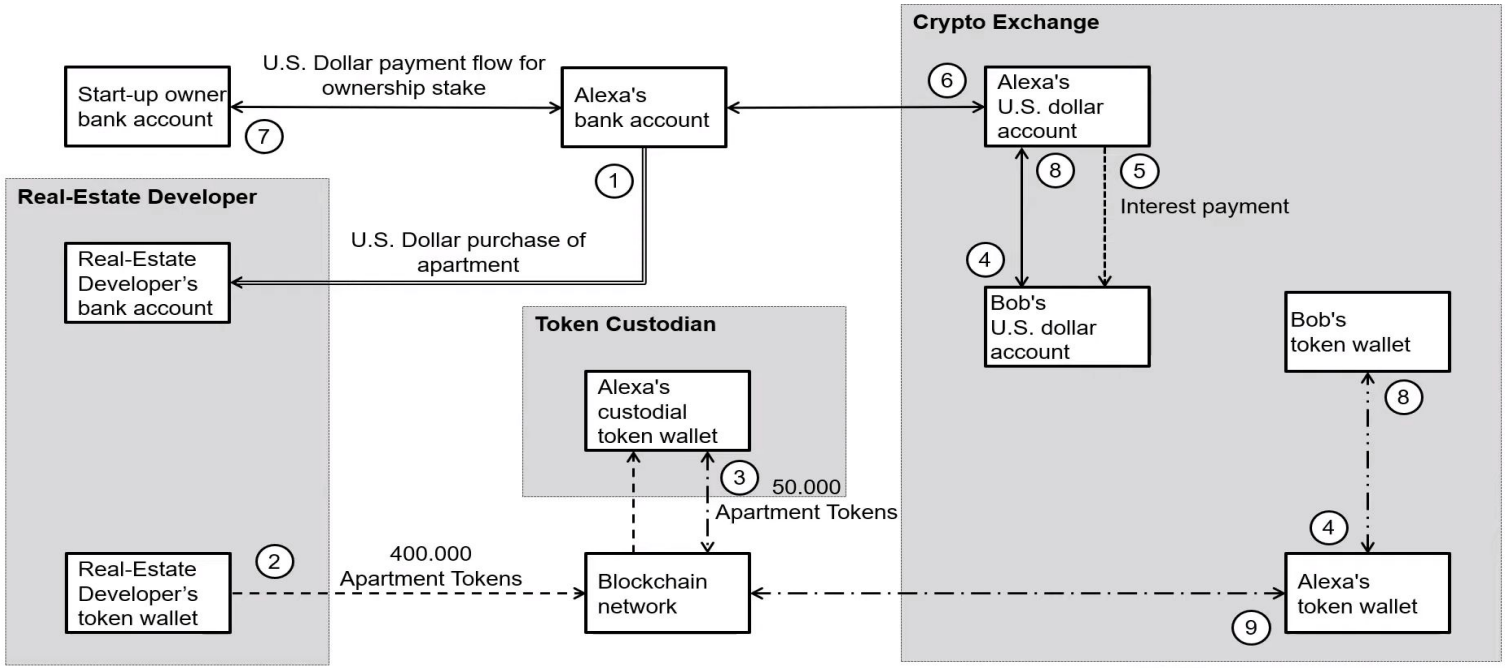
Investment: Diversification of investment portfolios with gold-backed tokens

Payments: Use of DGX tokens for transactions and remittances

Wealth Preservation: Hedging against inflation and economic uncertainties

Collateral: Utilization of DGX as collateral for loans and financial products

Case Studies:Real Estate: Fractional ownership of properties



Fungible Tokens:

- Refers to a type of digital asset that is interchangeable with another asset of the same type
- Fungible tokens are often used to represent assets such as currency, commodities, or other financial instruments on a blockchain (Bitcoin (BTC),Ethereum (ETH),USD Coin (USDC), Ethereum's ERC-20
- key characteristics and examples of fungible tokens:
    - Interchangeability
    - Indivisibility
    - Standardization
- Use Cases:

Fungible tokens have various use cases, including **digital currencies, stablecoins, loyalty points, and tokenized assets such as gold or real estate**. They can be traded on decentralized exchanges, used as a medium of exchange for goods and services, or utilized within decentralized finance (DeFi) applications for lending, borrowing, and liquidity provision.

ERC-20 is the **technical standard** for fungible tokens created using the Ethereum blockchain.

ERC-20 allows developers **to create smart-contract-enabled tokens** that can be used with other products and services. These tokens are a representation of an asset, right, ownership, access, cryptocurrency, or anything else that is not unique in and of itself but can be transferred.

ERC-20 Contents

ERC-20 is a list of functions and events that must be implemented into a token for it to be considered ERC-20 compliant. These functions (called methods in the ERC) describe what must be included in the smart-contract-enabled token, while events describe an action. The functions a token must have are:

- **TotalSupply**: The total number of tokens that will ever be issued
- **BalanceOf**: The account balance of a token owner's account
- **Transfer**: Automatically executes transfers of a specified number of tokens to a specified address for transactions using the token
- **TransferFrom**: Automatically executes transfers of a specified number of tokens from a specified address using the token
- **Approve**: Allows a spender to withdraw a set number of tokens from a specified account, up to a specific amount
- **Allowance**: Returns a set number of tokens from a spender to the owner

The events that must be included in the token are:

- **Transfer**: An event triggered when a transfer is successful
- **Approval**: A log of an approved event (an event)

The following functions are optional and are not required to be included, but they enhance the token's usability:

- Token's name (optional)
- Its symbol (optional)
- Decimal points to use (optional)

Non Fungible Tokens:

- Non-fungible tokens (NFTs) are a type of digital asset that represent ownership or proof of authenticity of a unique item or piece of content using blockchain technology
- Created, bought, sold, and traded on various blockchain platforms, etherium popular for NFT creation.
- unique characteristics and ownership history, providing transparency and authenticity to the digital asset.

Use Cases of NFTs

- Digital Art: Examples of NFTs representing digital artworks and their high-profile sales
- Collectibles: NFTs for virtual collectibles, trading cards, and rare items
- Gaming: Integration of NFTs in gaming for unique in-game assets and items
- Music and Media: NFTs for music albums, video clips, and other digital media.
- ERC721 is a standard for representing ownership of non-fungible tokens, that is, where each token is unique.

Challenges and Considerations

- Technological hurdles: need to scale to handle large volume of data.
- Ecosystem is still in early stage of development.
- Demand for experienced and custodian partners is not met.
- Legal and Regulatory Compliance: Compliance with securities laws, KYC/AML regulations, that need some form of centralization.
- Asset Valuation: Determining the value of tokenized assets
- Interoperability: Ensuring compatibility between different blockchain platforms and token standards
- Security Concerns: Risks of hacking, smart contract vulnerabilities

Future Trends

- Increased Adoption: Growing acceptance of tokenization as a means of asset representation
- Interoperability Solutions: Development of interoperability protocols for seamless asset transfer across different blockchains
- Regulatory Clarity: Continued efforts towards regulatory clarity and framework development
- Integration with DeFi: Integration of tokenized assets with decentralized finance (DeFi) protocols

Types of Tokens

- Tokens are classified according to the function and purpose
- Tokens serve various functions within blockchain ecosystems
- Different types of tokens catering to different use cases.

Types of tokens

1. **Transactional**: Tokens designed to be used as a payment method. Bitcoin is the most well-known of these.
2. **Utility:** XRP and ETH are two examples of utility tokens. They serve specific functions on their respective blockchains.
3. **Security tokens:** Tokens representing ownership of an asset, such as a stock that has been tokenized (value transferred to the blockchain). MS Token is an example of a securitized token. If you can find one of these for sale, you can gain partial ownership of the Millenium Sapphire.
4. **Governance:** These tokens represent voting or other rights on a blockchain, such as Uniswap.
5. **Non-Fungible Tokens (NFTs)**
6. **Stablecoins**
7. **Equity Token:**
8. **Wrapped Tokens**
9. **Tokenization Platforms:** These tokens support applications built to use a blockchain, such as Solana.

Transactional Tokens

Transactional tokens are used to transact—they serve as units of account and are exchanged for goods and services. These tokens often function like traditional currencies, but in some cases, provide additional benefits.

For example, with decentralized cryptocurrencies, such as Bitcoin and Dai, it is possible for users to execute transactions without a traditional intermediary or central authority, such as a bank or payment gateway. In addition to its function as a currency, Dai offers transactional performance to other networks. For example, POA Network created xDai, a Dai-like transactional token that lives on a sidechain, allowing for fast, inexpensive transactions.

Not all transactional tokens are currencies. Global supply chains and other industries utilize transactional tokens to apply the immutable nature of the blockchain and the flexibility of smart contracts to their operations.

Utility Tokens

https://www.gemini.com/cryptopedia/what-is-basic-attention-token-and-how-does-it-work Basic attention token on brave browser

https://trustmachines.co/glossary/utility-token/

https://www.ledger.com/academy/glossary/utility-token

https://www.coinsmart.com/articles/what-are-utility-tokens/

https://www.blockchain-council.org/blockchain/security-tokens-vs-utility-tokens-a-concise-guide/

Governance token

Tokenized equity

https://eqvista.com/cap-table/tokenized-equity/#:~:text=Example%20of%20tokenized%20equity&text=Quadrant%20Token%20was%20released%2C%20and,tokens%20at%20%241.25%20per%20token.

Supply and ownership

Custody

- The custody DeFi primitive refers to a decentralized finance (DeFi) component that focuses on the secure storage and management of digital assets within decentralized financial protocols.
- custody DeFi primitive entails:
  - Secure Storage:secure storage solutions for digital assets such as cryptocurrencies, tokens, and other blockchain-based assets.
  - Decentralization
  - Permissionless Access
  - Interoperability
  - Transparency and Audibility
- https://issanet.org/content/uploads/2023/10/Custody-Report_07.10.2023.pdf
- https://www.fireblocks.com/digital-asset-custody/

1. In escrow services, trusted banks are there to regulate the transactions. On the other hand, a smart contract is an automated contract wherein there is no regulatory authority.
2. In escrow, there is a third party that keeps the assets until the terms of the agreements are fulfilled. But, in the case of a smart contract, the contract itself holds the assets until the agreements are met.
3. Escrow usually functions in a centralized manner whereas a smart contract works in a decentralized manner adding more accountability.
4. The transaction fees in an escrow account are minimal whereas the transaction fees used to make the transactions based on a smart contract charge exorbitant gas fees.

SUPPLY ADJUSTMENT

- Supply adjustment applies specifically to fungible tokens and the ability to create (mint) and reduce (burn) supply via a smart contract.
- Burn: Reduce Supply

Burning a token means removing it from circulation and can be done in two ways: (1) manually send it to an unowned Ethereum address; or (2) even more efficiently, create a contract that is incapable of spending it.

- Mint: Increase Supply

Any mint mechanics have to be directly encoded into the smart contract mechanism.

Supply adjustment

Burn (reduce supply)

- To burn a token means to remove it from circulation.
- Burning a token can take two forms:
  - Manually send a token to an unowned Ethereum address.
  - More efficient is to create a contract that is incapable of spending them.
- Either approach renders the burned tokens unusable, although the decrease in circulating supply would not be "known" by the token contract. Burning is analogous to the destruction or irreversible loss of currency in the traditional finance world, which is unknown to the issuing government.

Supply adjustment

Why burn?

- Here are some practical reasons:
  - Represent exiting of a pool and redemption of underlying (common in equity tokens like cTokens for Compound)
  - Increase scarcity to drive the price upward (e.g., AAVE)
  - Penalize bad acting

Supply adjustment

Minting (increase supply)

- Minting increases the number of tokens in circulation.
- Contrary to burning, there is no mechanism for accidentally or manually minting tokens.
- Any mint mechanics have to be directly encoded into the smart contract mechanism.
- There are many use cases for minting as it can incentivize a wider range of user behavior.

Supply adjustment

Minting (increase supply)

- Here are some examples:
  - Represent entering a pool and acquiring corresponding ownership share (common in equity tokens like cTokens for Compound)
  - Decrease scarcity (increase supply) to drive the price downward (seigniorage Stablecoin models like Basis/ESD)
  - Reward user behavior

Supply adjustment

Minting as an incentive mechanism

- *Inflationary rewards* has become a common practice to encourage actions such as supplying liquidity or using a particular platform.
- Many users engage in *yield farming*, taking actions to seek the highest possible rewards. Platforms can bootstrap their networks by issuing a token with an additional value proposition in their network.
- Users can keep the token or sell it for a profit. Either way, utilization of the token benefits the platform by increasing activity.

Minting as a mechanism of incentive

1 Liquidity Provision: In decentralized exchanges (DEXs) and automated market maker (AMM) platforms like Uniswap, SushiSwap, or PancakeSwap, users can provide liquidity by depositing pairs of tokens into liquidity pools. When users deposit tokens into these pools, they receive LP (Liquidity Provider) tokens representing their share of the pool's liquidity. Minting occurs when these LP tokens are generated and distributed to users.

2 Yield Farming: Minting is also prevalent in yield farming protocols. In yield farming, users lock up or stake their tokens in smart contracts to earn rewards in the form of additional tokens. These rewards are often distributed in proportion to the amount of liquidity provided or tokens staked. When users stake their tokens and receive rewards, they are essentially "minting" new tokens as rewards for their participation.

3 Synthetic Assets: Some DeFi platforms allow users to mint synthetic assets, which are tokens that represent the value of real-world assets like fiat currencies, commodities, or stocks. Users can lock collateral (usually cryptocurrency) into smart contracts and mint synthetic assets against that collateral. These synthetic assets can then be traded or used within the DeFi ecosystem.

4 Algorithmic Stablecoins: Minting is also a key component of algorithmic stablecoins like DAI or TerraUSD. In these systems, new stablecoins are minted when the demand for the stablecoin increases. For example, when users deposit collateral into a smart contract, they can mint new stablecoins against that collateral, helping to maintain the stablecoin's peg to a target value (e.g., $1).

Supply adjustment

Bonding curves

- One advantage of being able to adjust supply up and down on a contractual basis is being able to define a bonding curve.
- A bonding curve is the price relationship between the token supply and a corresponding asset used to purchase the token(s).
- In most implementations investors sell back to the curve using the same price relationship.
- The relationship is defined as a mathematical function or as an algorithm with several clauses.

Supply adjustment

Linear bonding curves

- Let TKN to denote the price of a token denominated in ETH (which could be any fungible cryptoasset) and use *S* to represent the supply.
- The simplest possible bonding curve would be TKN=1 (or any constant).
- This algorithmically enforces a one to one peg between ETH and TKN

Supply adjustment

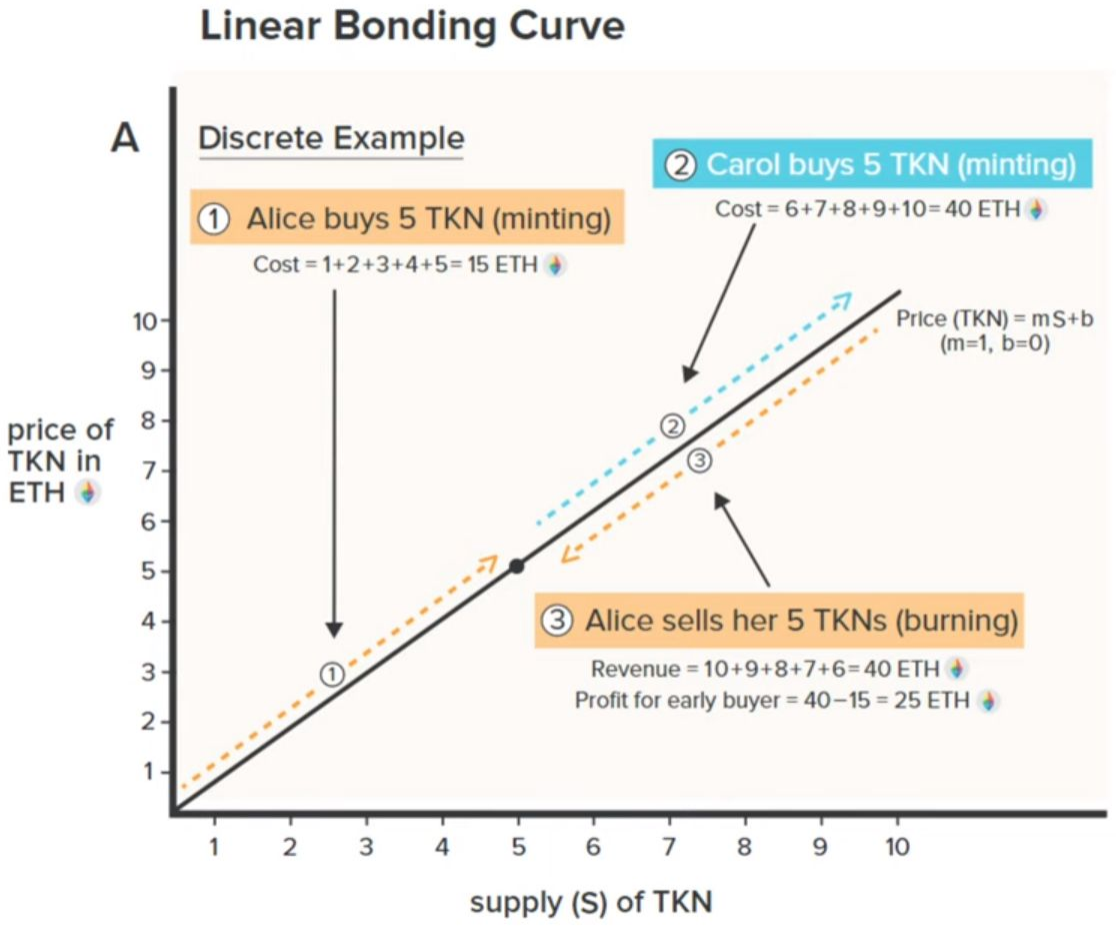
Linear bonding curves

- Next, consider a simple linear bonding curve, where m and b represent the slope and intercept, respectively, in a standard linear function.
- If $m = 1$ and $b = 0$, the first TKN would cost 1 ETH, the second would cost 2 ETH, and so on.
- A monotonically increasing bonding curve rewards early investors, because any incremental demand beyond their purchase price would allow them to sell back against the curve at a higher price point.

Supply adjustment

Linear bonding curves

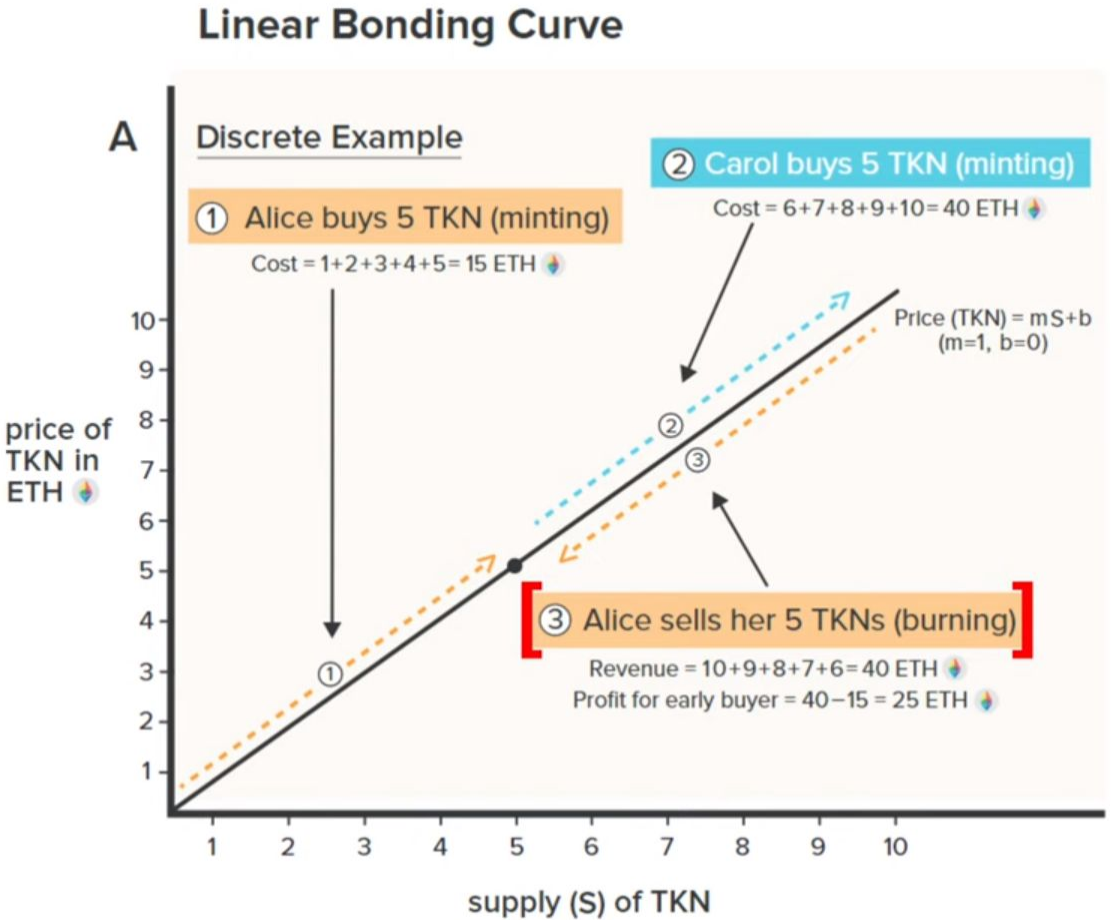
- Alice is rewarded for being an early investor



Supply adjustment

Linear bonding curves

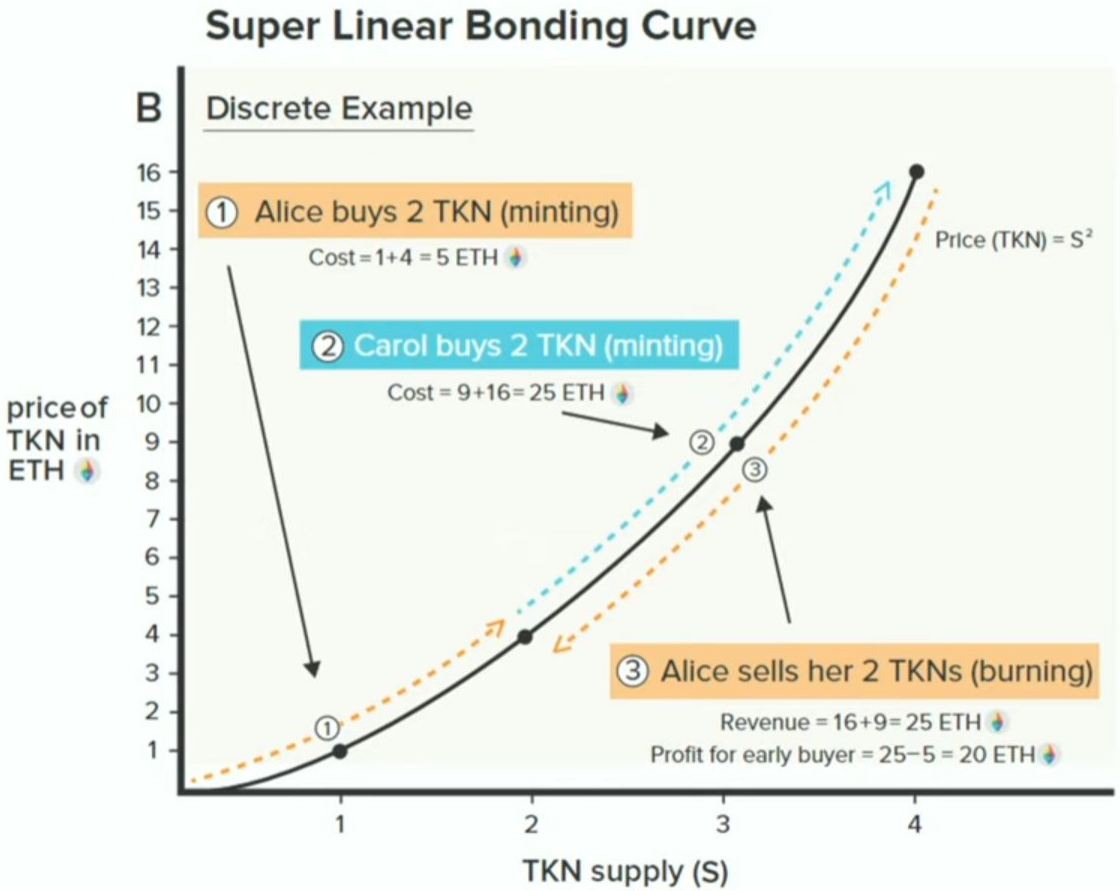
- Alice is rewarded for being an early investor



Supply adjustment

Super-linear bonding curves

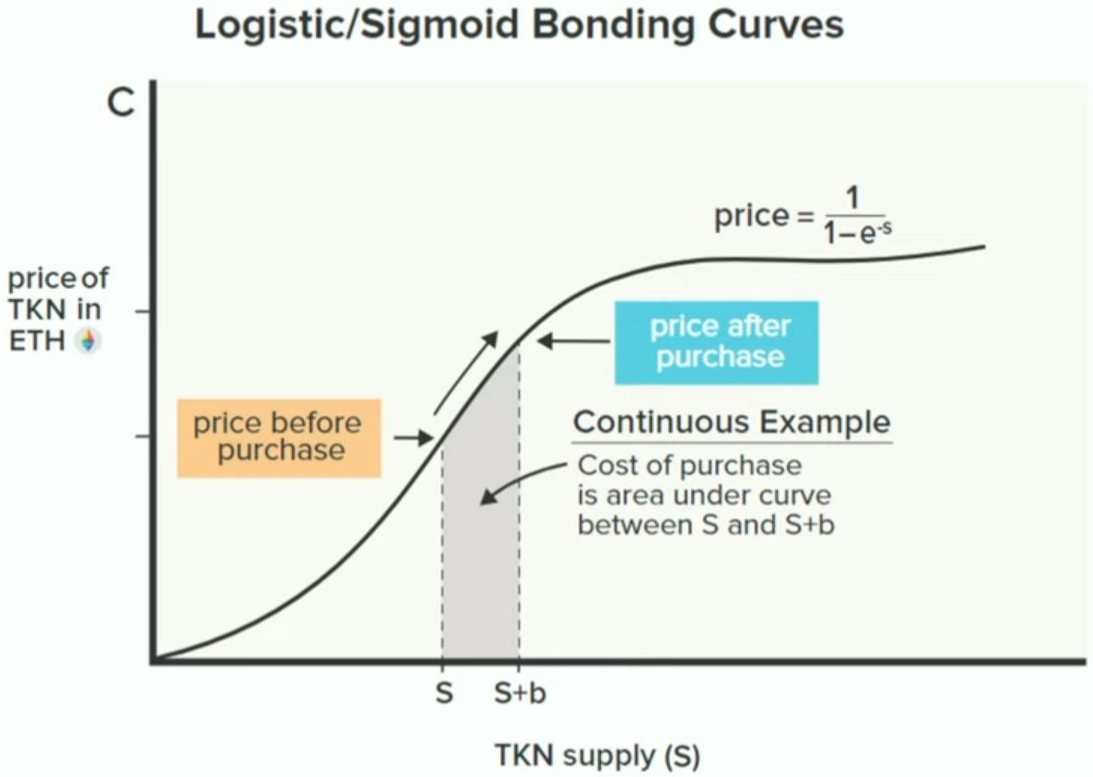
- Example: TKN = S^2
- More extreme rewards for early investors



Supply adjustment

Logistic bonding curves

- Rewards early but then flattens out



- Incentives

two different categories of incentives:

(1) staked incentives, which apply to a balance of tokens custodied in a smart contract; and

(2) direct incentives, which apply to users within the system who do not have a custodied balance

Incentives in DeFi refer to **design elements of the system that affect the behavior of system participants**[1]. These incentives are applied not only at the fundamental mechanisms of DeFi products, but also in the overall governance of the entire application which decides how these applications are developed[2].

Learn more:

Types of Cryptocurrency

For example,

Ethereum's ether was designed to be used as payment for validating transactions and opening blocks. When the blockchain transitioned to proof-of-stake in September 2022, ether (ETH) inherited an additional duty as the blockchain's staking mechanism.

Ripple's XRP is designed to be used by banks to facilitate transfers between different geographies.

Coin name and coin type are different

Payment Cryptocurrency

The purpose of a payment cryptocurrency, as the name implies, is not only as a medium of exchange but also as a purely peer-to-peer electronic cash to facilitate transactions. These payment cryptocurrencies also tend to have a limited number of digital coins that can ever be created, which makes them naturally deflationary. With less and less of these digital coins can be mined, the value of the digital currency is expected to rise.

Examples of payment cryptocurrencies include Bitcoin, Litecoin, Monero, Dogecoin, and Bitcoin Cash.

Disadvantages of defi

DeFi not only has properties that make it superior to traditional banking and finance, but it also allows for completely new applications. However, systems based on this new paradigm have weaknesses that ought to be addressed as such.
DeFi systems are currently still quite illiquid since only relatively few clients use these systems despite its outstanding growth rates. As a consequence, users are offered for instance less favorable prices on a DeX than on centralized trading platforms. Furthermore, DeFi systems are less scalable than centralized systems due to their peer-to-peer architecture (Chauhan, Malviya, Verma, & Mor, 2018). This sometimes leads to bottlenecks in the network, so-called “network congestions” (Yu et al., 2018), which can massively slow down business processes and render them more expensive (Chen & Bellavitis, 2020). Furthermore, compatibility problems still exist between DeFi platforms that are based on different blockchains. However, incorrectly programmed smart contracts could prove to be the greatest and most fundamental weakness of a DeFi system. If such an integral part of the system is incorrectly programmed and then runs automatically and unstoppably it can have fatal consequences for the entire system. Properties such as automatic, trustless and autonomous, which normally represent strengths, turn into vast disadvantages in the event of a malfunction.
These problems may then be amplified by the fact that no counterparty can be held responsible as the system is anonymous and permissionless (Zetzsche, Arner, & Buckley, 2020). It is even conceivable that perpetrators intentionally use such characteristics to scam credulous investors (Chohan, 2021)