GLOBAL MILLENNIAL CAPITAL

Decentralized Finance Technologies

Research and Insights White Paper

Public Information and Disclosure

Table of Contents

GLOBAL MILLENNIAL CAPITAL

01

Executive summary and key insights for our decentralized finance technologies research

Executive summary and key reflection points of our research study

Decentralized Finance (DeFi) is a fast-evolving sector that merges blockchain technology with financial services, aiming to bypass traditional intermediaries. Unlike traditional finance, DeFi services rely on smart contracts and open-source protocols, providing users with greater control through non-custodial wallets and decentralized governance systems. Key components of DeFi include digital assets, wallets, decentralized applications (dApps), and oracles, which allow off-chain data integration. This decentralized structure contrasts with traditional finance, which relies on intermediaries for asset custody, transaction execution, settlement, and governance.

Our research includes examination of prominent DeFi platforms Aave, Uniswap, Lido and dYdX that are exemplifying the innovation within the DeFi space, each addressing different needs in areas such as lending, staking, token swapping, and derivatives trading, while leveraging decentralized governance to re-think participation of users and other key stakeholders.

Even though DeFi addresses inefficiencies and risks inherent in traditional finance, challenges such as security vulnerabilities, over-collateralization requirements, and regulatory uncertainties persist. The decentralized nature of DeFi poses risks such as governance conflicts, anonymity in transactions, coding vulnerabilities and changes in regulatory perspectives. Regulatory challenges include difficulties in defining and classifying crypto assets across jurisdictions, compounded by the risks of money laundering and terrorism financing. While some regulatory frameworks are emerging, a unified global approach remains critical to mitigate risks and ensure financial stability.

Despite this, we remain optimistic on DeFi's potential to revolutionize financial markets and for it to continue gaining traction globally.

Our key predictions for DeFi technologies and business models

Cross Chain Bridging Interoperability

Prediction: Cross-chain bridging will become more advanced, allowing seamless movement of assets and data across multiple blockchain networks.

Implications: The ability to move assets and data freely between blockchains will create a more seamless and user-friendly experience, increasing DeFi adoption, especially among non-technical users.

Tokenization and Real-World Assets (RWA)

Prediction: Emerging web3 applications that utilizes real world assets in creative ways will expand financial possibilities for both TradFi and DeFi markets.

Implications: In decentralized finance (DeFi), RWA will introduce a more dependable asset base and greatly enhance the functionality of decentralized applications.

DeFi Insurance Products

Prediction: DeFi insurance products will aim to protect users against unforeseen losses, addressing the growing need for robust security measures as DeFi platforms become more sophisticated.

Implications: DeFi insurance protections will provide peace of mind to hesitant traders, potentially boosting trust and liquidity throughout the DeFi space.

Compliance and Regulatory Developments

Prediction: The regulatory environment for DeFi will become more stringent, with a focus on implementing Know Your Customer (KYC) and Anti-Money Laundering (AML) measures.

Implications: This will lead to greater institutional adoption of DeFi platforms, as compliance measures will help align DeFi with traditional financial systems.

Security and Risk

Prediction: Advanced smart contract auditing and enhanced risk assessment tools for users and investors will be crucial in ensuring the security and reliability of DeFi platforms.

Implications: Advanced cryptographic techniques, multi-signature wallets, and audits will become standard practices to safeguard user funds and data.

DeFi and AI Integration

Prediction: The use of AI and machine learning in DeFi is predicted to become more prevalent, enhancing functionalities like automated trading strategies, yield optimization and predictive analytics for market trends and user behavior.

Implications: AI algorithms can enhance risk assessment, automate decision-making processes, and optimize the execution of smart contracts for more efficient and secure transactions.

Our key predictions for DeFi technologies and business models (contd.)

Underlying Business Models

Lending and Borrowing

Description: Lenders can lend their cryptocurrencies or tokens to others in exchange for interest. Borrowers can take out loans by providing collateral.

Key Players: Compound, Aave

Revenue Stream: Liquidation fees, origination fees, interest rates

Decentralized Exchanges

Description: DEXs use AMM models to facilitate trading without requiring order books. Users provide liquidity to trading pools and earn fees from trades that occur within those pools.

Key Players: Uniswap, Sushiswap

Revenue Stream: Trading fees, liquidity provider fees, governance token incentives

Yield Farming and Staking

Description: Users can participate in DeFi activities and earn rewards from transaction fees, interest, or newly issued tokens. This model encourages users to lock up their assets for a period of time to earn higher returns.

Key Players: Yearn.finance, curve finance

Revenue Stream: Fees from yield, strategies and performance

Decentralized Insurance

Description: Users contribute to a pool of funds and can claim payouts in case of covered events, with decisions often governed by community voting.

Key Players: Nexus Mutual, Cover Protocol

Revenue Stream: Premiums, Claims fees, staking and governance fees

Derivatives and Synthetic Assets

Description: Such platforms allow users to create and trade synthetic assets that mirror the value of real-world assets like stocks, commodities, or fiat currencies. This model provides exposure to traditional assets without requiring direct ownership.

Key Players: Synthetic, dYdX

Revenue Stream: Trading, collateral and market making fees

Governance and Protocol

Description: Many DeFi platforms issue governance tokens that give holders voting rights on protocol changes, upgrades, and other decisions. Users can earn these tokens through participation in the network or by providing liquidity.

Key Players: MakerDAO

Revenue Stream: Governance appreciation tokens, staking and participation rewards

02

An overview of select decentralized finance (DeFi) ecosystems, underlying technologies and key applications

Key definitions and industry interpretations of DeFi (1/2)

General definition of decentralized finance technologies

Decentralized Finance (DeFi) technology is a broad term that encompasses a range of blockchain-based systems and applications designed to replicate, enhance, and democratize traditional financial services through decentralized networks. Unlike conventional financial systems that depend on centralized intermediaries such as banks, brokers, or payment processors, DeFi leverages decentralized platforms to provide financial services in a more open, transparent, and efficient manner.

Decentralized Finance (DeFi) technology represents a paradigm shift in the financial sector, utilizing blockchain and smart contracts to offer financial services that are decentralized, transparent, and accessible. By removing intermediaries and leveraging open-source protocols, DeFi aims to create a more inclusive and efficient financial ecosystem.

Definition by practitioners of decentralized finance technologies

Practitioners of DeFi, contribute by developing and securing DeFi technologies, ensuring compliance with regulations, enhancing user experience, engaging with the community, and providing financial analysis. Their collective efforts drive the innovation, security, and adoption of DeFi, ultimately shaping the future of decentralized financial systems.

Key definitions and industry interpretations of DeFi (2/2)

DeFi is an innovative approach to financial services that utilizes decentralized networks and smart contracts to provide financial products and services.
- Stani Kulechov (Founder of Aave)

DeFi refers to a set of applications and services built on Ethereum and other blockchain platforms that aim to provide financial services in a decentralized manner. These applications use smart contracts to automate financial operations and eliminate the need for traditional intermediaries, thus enabling open, transparent, and permissionless financial systems.
- Vitalik Buterin (Ethereum co-founder)

Defi involves creating decentralized alternatives to traditional financial systems, such as decentralized exchanges, lending protocols, and yield farming platforms, enabling users to interact directly with these services.
- Hayden Adams (Founder of Uniswap)

Decentralized Finance (DeFi) encompasses a range of financial services and products that are built on blockchain technology and operate without intermediaries.
- Robert Leshner (Founder of Compound)

General overview of decentralized finance

DeFi encompasses a variety of activities and business relationships, each characterized by fundamental attributes that define the structure of the DeFi ecosystem and its emerging developments. Key DeFi service categories include stablecoins, exchanges, credit, derivatives, insurance, and asset management, as well as auxiliary services such as wallets and oracles. Unlike traditional finance, which relies on intermediaries to manage and process financial services, DeFi operates in a decentralized environment using public, permissionless blockchains. Services which are generally encoded in open-source software protocols and smart contracts.

DeFi leverages blockchain technology to facilitate alternatives to traditional service providers and market structures. It offers the potential for innovation and the creation of new services that improve the efficiency of financial markets, building upon work being done in financial technology (fintech) and blockchain technology more broadly.

An overview of defining characteristics of decentralized finance

Characteristics of decentralized finance

DeFi takes advantage of various technologies developed in the blockchain sphere. While these technologies have applications outside of DeFi, they play essential roles within the DeFi ecosystem:

Blockchains
Description: Distributed ledgers serving as the settlement layer for transactions. Most DeFi services currently operate on the Ethereum network due to its capabilities and developer adoption. However, DeFi activity is growing on and across other blockchains as well.

Digital Assets
Description: Tokens representing value that can be traded or transferred within a blockchain network. Bitcoin and other cryptocurrencies were the first blockchain-based digital assets, but others have a range of intended functions beyond payments.

Wallets
Description: Software interfaces for users to manage assets stored on a blockchain. With a non-custodial wallet, the user has exclusive control of funds through their private keys. Custodial wallets, on the other hand, have private keys managed by a service provider.

Smart Contracts
Description: Blockchain-based software code that executes, controls, and documents relevant events and actions according to predefined terms and rules.

Decentralized Autonomous Organizations
Description: Entities whose rules are defined and enforced in the form of smart contracts.

Decentralized Applications (dApps)
Description: Software applications built out of smart contracts, often integrated with user-facing interfaces using traditional web technology.

Governance Systems
Description: Software-based mechanisms that manage changes to smart contracts or other blockchain protocols, often based on tokens that allocate voting rights to stakeholders.

Stablecoins
Description: Digital assets whose values are pegged to a fiat currency, a basket of fiat currencies, or other stable-value assets.

Oracles
Description: Data feeds that allow information from sources off the blockchain, such as the current price of a stock or a fiat currency, to be integrated into DeFi services.

An overview of differentiators and benefits of decentralized finance

Contrasting elements of a decentralized finance ecosystem

DeFi presents a stark contrast to traditional finance in several ways:

- **Custody of Assets:** In traditional finance, assets are held by a regulated service provider or custodian on behalf of asset owners. In DeFi, assets are held directly by users in non-custodial wallets or via smart contract-based escrow.
- **Units of Account:** Traditional finance typically uses fiat currency as the unit of account. In DeFi, units are denominated in digital assets or stablecoins, which may themselves be pegged to fiat money.
- **Execution:** Traditional finance relies on intermediaries to process transactions between parties. In DeFi, transactions are executed via smart contracts operating on the user's assets.
- **Clearing and Settlement:** Traditional finance uses service providers or clearinghouses to process and settle transactions, often after a period of time. In DeFi, writing transactions to the underlying blockchain completes the settlement process.
- **Governance:** In traditional finance, governance is specified by the rules of the service provider, marketplace, regulator, or self-regulatory organization. In DeFi, governance is managed by protocol developers or determined by users holding tokens granting voting rights.
- **Auditability:** Traditional finance may involve authorized third-party audits of proprietary code or open-source code that is publicly verified.

In DeFi, open-source code and a public ledger allow auditors to verify protocols and activity.

- **Collateral Requirements:** Traditional financial transactions may involve no collateral or collateral equal to or less than the funds provided. DeFi generally requires overcollateralization due to digital asset volatility and the absence of credit scoring.
- **Cross-Service Interaction:** Traditional finance has limited cross-service interaction, moving toward Open Finance via application programming interfaces (APIs) or dedicated intermediaries. DeFi services can integrate with any other service on the same blockchain and potentially across chains.
- **Access and Privacy:** Traditional finance conducts identity checks and personal data management according to national privacy laws. DeFi is still discussing identity verification requirements with anti-money laundering regulators, with user balances and transaction activity generally being public.
- **Security:** Both traditional finance and DeFi are vulnerable to hacks and technical risks, but the mechanisms and responses differ.
- **Investor Protection:** Traditional finance involves government-mandated disclosures and consumer protections. In DeFi, users assume all risks, though private redress arrangements such as DeFi insurance offer some protection against losses.

Decentralized finance definition and ecosystem overview

Decentralized Finance (DeFi) refers to a novel financial system that operates on decentralized blockchain technology, primarily using Ethereum. Unlike traditional financial systems, DeFi eliminates intermediaries like banks and brokers, allowing for peer-to-peer transactions and the creation of decentralized applications (dApps). The DeFi ecosystem includes a variety of financial services such as lending, borrowing, trading, and investing.

Key components of this ecosystem include:

01

DECENTRALIZED EXCHANGES

Platforms like Uniswap and Sushiswap that allow users to trade cryptocurrencies directly with one another without the need for a centralized authority.

02

LENDING AND BORROWING PLATFORMS

Services like Aave and Compound where users can lend their cryptocurrencies to earn interest or borrow against crypto assets.

03

STABLECOINS

Cryptocurrencies like DAI and USDC that are pegged to stable assets like the US dollar to reduce volatility.

04

YIELD FARMING AND STAKING MECHANISMS

Mechanisms that allow users to earn rewards by providing liquidity or staking their crypto assets in various protocols.

05

DEFI INSURANCE PROTOCOLS

Decentralized insurance protocols like Nexus Mutual that offer coverage against risks in the DeFi space.

Key applications and characteristics of Decentralized Finance

Decentralized finance key characteristics

Not every application of blockchain technology—even those involving financial transactions—can be classified as DeFi. Nor is every element contributing to the DeFi ecosystem appropriately considered a DeFi service, business, or software protocol. While the space is evolving, certain distinguishing characteristics define DeFi:

- **Financial Services:** DeFi directly mediates the transfer and exchange of value. Auxiliary services such as oracles, query systems, and decentralized storage are important enablers of DeFi activity but should be distinguished from DeFi services themselves.
- **Trust-Minimized Operation and Settlement:** DeFi projects generally build on public, permissionless blockchains offering smart contract functionality, such as Ethereum. Transactions are executed and recorded according to the rules of the DeFi protocols. Trust minimization often extends to the governance structures that establish the conditions for protocol changes.
- **Non-Custodial Design:** The assets issued or managed by DeFi services cannot be unilaterally expropriated or modified by third parties, even those providing intermediation and other services. Users retain full control, meaning centralized cryptocurrency exchanges with custody over digital assets are not DeFi businesses, though many are developing DeFi offerings.
- **Open, Programmable, and Composable Architecture:** There is broad availability of the underlying source code and a public application programming interface (API). Components can be composed together and programmed to create new financial instruments and services dynamically. For example, a stablecoin may be used as the foundation for a derivative, which is then used as collateral on a loan and subject to an insurance contract.

An overview of decentralized finance infrastructure overview

Decentralized Finance (DeFi) represents a transformative shift in the financial landscape, offering a more transparent, accessible, and open financial ecosystem. By leveraging blockchain technology and smart contracts, DeFi eliminates the need for traditional intermediaries, reducing costs and increasing efficiency. The various components of the DeFi ecosystem—DEXs, lending and borrowing platforms, stablecoins, yield farming and staking, and insurance—each play a crucial role in building a robust and decentralized financial system. While challenges remain, the rapid innovation and growing adoption of DeFi highlight its potential to revolutionize finance and empower individuals worldwide. The DeFi infrastructure comprises various layers and components that work together to facilitate decentralized financial services.

Blockchain Layer

The foundational layer, primarily represented by Ethereum, which hosts the majority of DeFi applications. Other blockchains like Binance Smart Chain and Solana are also gaining traction.

Protocol Layer

This layer includes the smart contracts and protocols that define the rules and operations of DeFi services. Examples include the ERC-20 token standard and the various DeFi protocols like Uniswap (for trading) and MakerDAO (for stablecoin issuance).

Application Layer

The front-end interfaces and dApps that interact with the underlying protocols. These are the platforms that users interact with directly, such as Metamask for wallets and Compound for lending/borrowing.

Aggregation Layer

The tools and services that combine multiple DeFi protocols to provide enhanced functionalities and user experience. Examples include yield aggregators like Yearn Finance and DEX aggregators like 1inch.

An overview of decentralized finance models for key stakeholders

The convergence of retail and institutional DeFi is fostering a more cohesive financial ecosystem. Innovations initiated in retail DeFi are being scaled up to meet institutional demands, while institutions are adapting these innovations to create more advanced financial products and services. This dynamic interplay is expected to drive further growth in DeFi.

DeFi Models for Retail

Designed for individual users who engage in DeFi for personal financial activities. Key features include:

- Autonomy: Users maintain control over their own wallets and private keys with personal management of assets without relying on any third party or custodian intermediaries.
- Financial Inclusion: DeFi provides financial services to individuals without access to traditional banking, breaking down barriers with minimal entry requirements.
- Accessibility and User-Friendly Interfaces: Users can access a variety of financial services directly from their smartphones and manage assets through decentralized applications (DApps) on blockchains. These platforms are designed to be accessible and easy to use for non-technical users.
- Innovative Financial Products: There's a range of products including yield farming, staking, and decentralized exchanges.
- Small-Scale Transactions: Typically involve smaller amounts of capital.
- Community Governance: Many DeFi projects are governed by their communities through mechanisms like DAOs, where changes to protocols are voted on by token holders.

DeFi Models for Institutional

Cater to larger financial institutions, hedge funds, and corporate entities. Key features include:

- Advanced Security and Compliance: Higher emphasis on regulatory compliance, security measures, and risk management.
- Large-Scale Transactions: Facilitate significant volumes of transactions and large capital movements.
- Higher Returns: Institutional platforms provide access to DeFi lending and yield farming protocols, offering returns that exceed those in traditional finance.
- Integration with Traditional Finance: Often integrate with traditional financial systems and offer tailored solutions for institutional needs, such as custody services and advanced trading tools.
- Permissioned Layers: Some DeFi platforms offer private, permissioned layers where all participants are vetted, creating a secure and compliant environment for regulated entities.

Select economic benefits of DeFi applications (1/2)

Economic Benefit	Particulars
Cost Reduction	DeFi applications often have lower transaction fees compared to traditional financial services, as they eliminate intermediaries like banks and payment processors. This reduction in fees can lead to significant cost savings for users.
Enhanced Liquidity	DeFi enables the tokenization of assets, allowing for fractional ownership and more liquid markets. This increases the ability to buy, sell, and trade smaller portions of high-value assets. DEXs provide continuous trading opportunities and liquidity without relying on centralized order books, which helps to reduce trading costs and improve market efficiency.
Transparency	Transactions and smart contract operations are recorded on a public blockchain, providing transparency and a verifiable history of financial activities. This transparency helps build trust among users and reduces the potential for fraud.
Speed and Efficiency	DeFi transactions can be executed rapidly, often within minutes, compared to the slower processing times of traditional financial systems. DeFi platforms operate round-the-clock, allowing users to conduct financial activities at any time without the constraints of traditional banking hours.

Select economic benefits of DeFi applications (2/2)

Economic Benefit	Particulars
Decentralized Governance	DeFi applications often use governance tokens to allow stakeholders to participate in decision-making processes. This decentralized governance model ensures that changes and upgrades are made based on community input and consensus.
Investment Opportunities	DeFi platforms offer opportunities for users to earn returns on their assets through yield farming and staking. By providing liquidity or staking tokens, users can earn rewards or interest.
Token Incentives	DeFi applications often use tokens to align the interests of users, liquidity providers, and developers. Incentives may include reward programs, staking incentives, and governance voting rights.
Financial Inclusion	Traditional financial services often require high minimum investment amounts or stringent credit checks. DeFi platforms often allow smaller investments and lower requirements for participation, making financial services more accessible.

Utility of smart contracts for Decentralized Finance applications

Understanding Smart Contracts

The emergence of Decentralized Finance (DeFi) has revolutionized the traditional financial sector by utilizing blockchain technology to offer innovative and self-governing financial solutions. At the heart of this transformation are smart contracts, which play a crucial role in automating and securing various financial processes within the DeFi ecosystem. DeFi leverages Smart Contracts to unlock multiple use cases, such as borrowing, lending, trading, and derivatives. It is built on the composability principle, as it can combine different Smart Contracts to create new financial instruments. Smart contracts are the foundation that enables DeFi development to provide more efficient, transparent, and accessible financial services. They will play a significant role in the success of DeFi in the future.

Smart contracts are automated, self-executing agreements with the terms directly embedded into code. They operate on blockchain networks, allowing predefined actions to be executed automatically when specific conditions are met. The concept, first proposed by computer scientist and cryptographer Nick Szabo in the 1990s, gained widespread implementation with the advent of blockchain platforms like Ethereum. They are used to automate contract execution so that all participants are assured of the outcome without intermediaries.

Some of the key benefits of Smart Contracts include i) cost reduction and other formalities without compromising credibility ii) trust and transparency improvements due to lack of intermediaries and iii) reduction of fees and delays.

An overview of the utility of Smart Contracts for DeFi applications

Lending and Borrowing Contracts

These contracts enable direct peer-to-peer lending and borrowing, bypassing traditional financial intermediaries. They handle terms, interest rates, collateral requirements, and automatic loan execution. Examples include Compound and Aave that utilize these contracts to facilitate asset lending and borrowing.

Decentralized Exchange (DEX) Contracts

DEX contracts allow users to trade cryptocurrencies directly without relying on centralized exchanges. They manage order matching, fund custody, and trade settlements in a decentralized and automated manner. Examples include Uniswap and SushiSwap that use these contracts for cryptocurrency swaps.

Yield Farming Contracts

These contracts manage reward distribution and complex mechanisms to incentivize liquidity provision. They optimize strategies across multiple DeFi protocols to maximize returns for users. Examples include Yearn.finance which employs these contracts for yield optimization.

Insurance Contracts

DeFi insurance contracts offer protection against risks such as smart contract failures or protocol issues. They define insurance policy terms, premium payments, and automated payouts for covered events. Examples include Nexus Mutual uses these contracts to provide coverage against smart contract vulnerabilities.

Decentralized Infrastructure

They leverage blockchain networks to remove intermediaries, ensuring a transparent and secure financial system with no central control.

Coding and Execution

Written in programming languages like Solidity, smart contracts have immutable code once deployed, defining the rules and conditions of agreements.

Tokenization of Assets

They facilitate the creation of digital tokens representing real-world assets, enabling fractional ownership and broader market participation.

Oracle for Real-World Data

They rely on oracles to provide real-time data, such as asset prices or interest rates, which are essential for executing contract functions accurately.

03

Decentralized finance infrastructure and key ecosystem participant's overview

An overview of decentralized finance market mechanism (1/3)

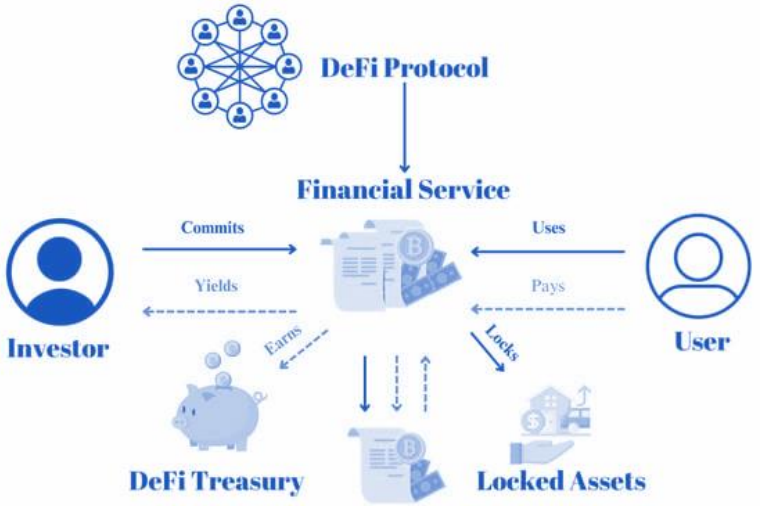
An overview of DeFi market mechanism

DeFi protocols provide services like exchanges, lending, and asset management. Decentralized exchanges (DEXs) facilitate on-chain token trades. The DeFi market employs automated market makers (AMMs) for asset pricing and control. The DeFi business model revolves around smart contracts, investors, and users engaging in asset movements and generating revenue for the DeFi treasury.

Two primary DEX order systems exist i) centralized order systems and ii) automated market makers. AMMs employ algorithms to ascertain asset prices, minimizing environmental uncertainty and information asymmetry. They furnish pricing with signaling value, providing generalized asset value information for both buyers and sellers. DeFi operates on a market mechanism, empowering users with control over and the capability to modify various assets using DeFi services.

The DeFi protocol generates financial services with a percentage of investors and users supporting these services. This process ultimately results in the creation of the DeFi treasury and the locking of assets.

Graph: A common mechanism of the DeFi business model.



An overview of decentralized finance market mechanism (2/3)

An overview of DeFi market mechanism

Protocol: A collection of smart contracts encompassing various facets like PLFs, AMMs, or yield aggregators. These protocols offer open, noncustodial, permissionless, and composable financial services in exchange for nominal fees levied on asset movements, such as borrowing or swapping.

Investor: This participant assumes the underlying protocol risk, including potential misbehavior, impermanent loss, or rug-pulls, in return for passive income. Their primary role involves depositing assets and providing liquidity to these financial services.

User: Typically, users interact with the protocol in real time, not expecting extended responses. However, in the case of yield aggregators, users may also function as investors. Users initiate asset movements and pay interest rates to the protocol.

Financial Service: The linchpin of the entire protocol, this entity locks assets, fulfills asset movement requests, and safeguards against protocol misuse. Additionally, it can act as an investor by leveraging other DeFi protocols, ultimately delivering yields and earnings to other participants.

Smart Contract Role in DeFi

Smart contracts in DeFi have the ability to automate financial transactions and eliminate the need for intermediaries. Rooted in blockchain technology, smart contracts are digital agreements operating within a decentralized framework, eliminating the requirement for third-party involvement. These programmable contracts autonomously enforce predetermined conditions and actions, reducing transaction costs, enhancing efficiency, and improving transparency. Within a smart contract, variables can be adjusted based on the logic programmed into its function. Once created, a smart contract can be executed on a blockchain network and applied to any participant within the network. These smart contracts facilitate unalterable and globally enforceable agreements between parties due to their synchronized record. The code of a smart contract self-executes once it fulfills the agreed-upon conditions. DeFi heavily relies on smart contracts because they play a pivotal role in ensuring the security and integrity of the DeFi ecosystem. Furthermore, within the DeFi landscape, smart contracts can be leveraged to generate profits from locked assets by utilizing perpetual contract NFTs, which represent the rights associated with a perpetual contract and its collateral.

An overview of decentralized finance market mechanism (3/3)

An overview of DeFi market mechanism

Peer-to-Peer Transaction in DeFi

The peer-to-peer (P2P) transaction mechanism plays a vital role in ensuring transactions and data privacy. In the context of blockchain transactions and DeFi, including exchange and payment, P2P typically involves a two-step process. Initially, involved parties negotiate and agree on exchange rates for specific pairs of crypto assets. Subsequently, these transactions are executed on-chain using smart contracts. P2P systems hold significant importance in enabling DeFi by facilitating direct trading of crypto assets between users. This approach reduces transaction costs and enhances liquidity within the DeFi ecosystem. By eliminating the need for intermediaries, P2P transactions enhance the overall efficiency and accessibility of DeFi platforms, contributing to the growth and success of the DeFi space.

Tokenization Mechanism

Tokenization digitizes assets, representing ownership on a blockchain network. It encompasses a wide range of assets, including commodities and real estate, and enhances market efficiency by enabling direct participant interactions. Tokenization is evolving in markets like commodities and real estate, thereby presenting new opportunities in direct lending and DeFi markets. Blockchain ensures the security of these tokens, which is vital in tokenizing real assets. This practice is gaining traction, especially in collateralizing real-world assets (RWAs) and aiding risk management. Tokenized asset ownership embedded within the system allows easy access to transaction records and identification of buyers and sellers. Tokenization has the potential to revolutionize traditional custody and settlement models by enabling direct interactions among market participants in a trustless environment. This disintermediation enhances market efficiency and grants investors access to otherwise illiquid assets. It finds applications in commodities, debt and equity securities, and real estate markets.

The role of blockchain technology in the financial industry (1/2)

Blockchains

Blockchain technology has significantly contributed to modernizing finance, gaining recognition within the banking sector for its potential to bolster transaction security and foster financial market development. Through decentralized operations, blockchain instills heightened confidence in previously centralized systems, establishing trustless networks where parties transact without relying on mutual trust. Immutable transaction records ensure both security and transparency, driving their widespread adoption across diverse industries.

The decentralized and secure nature of blockchain has rendered it accessible and cost-effective, particularly benefiting unbanked and underbanked individuals, thereby promoting financial inclusion. The advent of Bitcoin, coupled with blockchain, revolutionized financial transactions by eliminating the need for mutual trust. Moreover, blockchain's applications extend beyond finance to encompass distributed cloud storage, smart property, supply chain management, healthcare, and decentralized autonomous organizations (DAOs). Blockchain adoption facilitates secure and transparent data storage, facilitating financial transactions among entities that lack trust without necessitating a central trusted third party. In the realm of decentralized finance (DeFi), supported by blockchain and smart contracts, peer-to-peer transactions thrive. For instance, Ethereum, as a permissionless blockchain, facilitates decentralized and inclusive participation for all stakeholders.

Decentralized finance (DeFi) represents a novel paradigm that fundamentally transforms the creation, distribution, and utilization of financial services. In the realm of DeFi, software is distributed in a decentralized manner across networks, ushering in a new era of open financial infrastructure. By harnessing blockchain technology, DeFi protocols facilitate various transactions within their systems, including loans, stablecoin, tokenization, asset management, payment, insurance, staking, and exchanges. These protocols establish a decentralized and inclusive financial infrastructure, offering global access to self-sovereign and censorship-resistant financial services. Consequently, DeFi is more flexible and accessible than TradFi.

Blockchain technology role in enabling decentralized finance (DeFI)

DeFi

Decentralized finance (DeFi) represents a novel paradigm that fundamentally transforms the creation, distribution, and utilization of financial services. In the realm of DeFi, software is distributed in a decentralized manner across networks, ushering in a new era of open financial infrastructure. By harnessing blockchain technology, DeFi protocols facilitate various transactions within their systems, including loans, stablecoin, tokenization, asset management, payment, insurance, staking, and exchanges. These protocols establish a decentralized and inclusive financial infrastructure, offering global access to self-sovereign and censorship-resistant financial services. Consequently, DeFi is more flexible and accessible than TradFi. DeFi offers significant advantages, as stated in the following points:

1. DeFi can potentially reduce transaction costs and offer alternatives to traditional financial intermediaries.
2. Through DeFi-based financial services, individuals can connect directly with one another, enabling more affordable and accessible access to basic financing.
3. DeFi facilitates secure crypto asset transfer and management, granting users control and transparency over their financial assets.
4. DeFi's composability allows for the assembly of building blocks to create novel services, such as stablecoins for yield farming and generating returns.
5. DeFi tokens in the market display varying degrees of efficiency, with many investors acquiring them for their utility rather than solely for speculative purposes

Blockchain technology role in enabling tradFi and CeFi

TradFi

TradFi represents the conventional non-blockchain financial system. Centralized finance (CeFi) acts as a centralized intermediary between TradFi and DeFi. DeFi, built on blockchain technology, offers flexibility and higher potential returns but also poses unique risks and challenges within the decentralized financial sector.

TradFi denotes traditional finance entities operating outside blockchain systems, engaging in activities like asset management, insurance, and real estate funds. Dealing exclusively with fiat and traditional assets, TradFi is known and recognized for its user-friendly experiences and stringent strict regulation.

CeFi

CeFi offers crypto services within a centralized structure. Platforms like Binance, Coinbase, Gemini, Kraken, and Nexo serve as these intermediaries, providing services like fiat-to-crypto conversion and customer support. Despite benefits like regulatory compliance and simplified DeFi services, CeFi platforms face drawbacks like higher costs and custody issues. They are popular for users seeking regulated crypto market access.

CeFi encompasses cryptocurrency exchanges and shares similarities with TradFi, featuring advantages and disadvantages. Central bank digital currencies (CBDCs) play a pivotal role in reinforcing CeFi due to their digital nature and issuance by the central bank. CBDCs are digital versions of a nation’s fiat currency, directly backed and regulated by the government. In contrast, CeFi refers to traditional financial services for cryptocurrencies, relying on centralized intermediaries for transactions. These services include lending, borrowing, and trading, typically offered by centralized financial institutions or platforms.

Participants within a decentralized finance network overview

Despite the previous downturns in the cryptocurrency market, the underlying infrastructure of Web3 remains solid, with ongoing developments that promise significant enhancements to DeFi systems. These advancements underline the potential of DeFi to sustain growth and innovation that can be independent of market volatilities. By distributing data across a blockchain, DeFi ensures that no single entity can control or manipulate the system. This framework reduces risks like fraud and data tampering and gives users unprecedented control over their financial transactions and data.

Blockchain

Blockchain technology acts as a public, distributed ledger that records all transactions across a network of computers. This decentaralization eliminates single points of failure, enhancing the efficiency and security of financial transactions.

Smart Contracts

Self-executing contracts with the terms of the agreement written in lines of code. Governed by decentralized autonomous organizations (DAOs), smart contracts execute automatically based on underlying conditions, therefore reducing the need for intermediaries and enhancing transaction efficiency.

Digital Assets

DeFi utilizes various forms of digital assets, including cryptocurrencies, non-fungible tokens (NFTs), and tokenized real-world assets. These assets provide a wide range of functionalities from value transfer to representing ownership of physical or digital goods.

Select properties of a standard decentralized finance protocol

Decentralized Finance (DeFi) protocols are built on blockchain technology to provide financial services in a decentralized and automated manner. These properties collectively define the DeFi ecosystem, highlighting its innovative approach to providing financial services through decentralized, transparent, and programmable means.

Decentralization

DeFi protocols operate on a decentralized network of nodes rather than being controlled by a single entity or central authority. This structure ensures that no single party has complete control over the protocol, enhancing security and reducing the risk of central points of failure

Transparency

Transactions and activities within DeFi protocols are recorded on a public blockchain ledger. This openness allows participants to verify and audit transactions independently, promoting trust and accountability. Many DeFi protocols are open-source, meaning their code is available for anyone to review and contribute to. This transparency fosters trust and enables community-driven improvements and security audits.

Interoperability

Many DeFi protocols are designed to work seamlessly with other DeFi services and applications. This interoperability allows for the creation of complex financial ecosystems where various protocols and tools can interact and exchange value.

Governance

Many DeFi protocols include governance mechanisms that allow stakeholders to participate in decision-making processes. Governance tokens or voting systems enable users to propose and vote on changes or upgrades to the protocol.

04

Cryptocurrencies and digital assets ecosystem overview

Cryptocurrencies and digital assets high level overview

An overview of cryptocurrencies and digital assets ecosystem

Digital assets like cryptocurrencies, NFTs and other tokens have emerged into a very significant trend. Ethereum's utility, particularly its smart contract capabilities and support for decentralized finance (DeFi), non-fungible tokens (NFTs), and decentralized applications (dApps), has attracted institutional interest due to its numerous real-world applications. Financial institutions increasingly view blockchain-based transactions as faster, cheaper, and safer than traditional banking systems. The adoption of crypto and blockchain technology, especially for cross-border payment solutions, offers efficient and cost-effective transaction alternatives.

Blockchains are the technology solutions that enable digital assets. A blockchain is a method of securely recording information on a peer-to-peer network. It’s a shared public database, duplicated across computer systems, in which new entries can be added but existing entries can’t be altered.

Blockchain entries, called blocks, are generated via specific protocols that are different for each blockchain. Each block contains encoded information about the previous block, reinforcing the order and structure of the blockchain as it grows.

A digital asset is created, or minted, when new information is added to a particular blockchain. Through blockchain entries, users can exchange existing digital assets and/or create new (mint) ones.

Key benefits for the adoption of cryptocurrencies and digital assets

Key benefits of institutional adoption of cryptocurrencies and digital assets

Institutional adoption of cryptocurrencies, especially Bitcoin or Ethereum, has surged in recent years due to several key factors:

Recognition as an Asset Class: Institutional investors, hedge funds, and asset managers view Bitcoin and Ethereum as legitimate asset classes, akin to gold or other commodities, increasingly as stores of value and investment assets.

Diversification: Investments in cryptocurrencies like Bitcoin and Ethereum enable institutional investors to diversify their portfolios, potentially improving risk-adjusted returns due to low correlation with traditional asset classes.

Institutional Infrastructure: The development of regulated investment vehicles such as Bitcoin futures, ETFs, and other institutional-grade infrastructure like cryptocurrency exchanges and derivatives markets has facilitated secure institutional investments in cryptocurrencies.

Macroeconomic Uncertainty: Factors such as inflation, geopolitical instability, and currency devaluation underscore the need for institutional investors to seek alternative stores of value and hedges against traditional financial risks. Bitcoin is often cited as a hedge against inflation due to its fixed supply and decentralized nature.

Regulatory Clarity: Developments like the approval of Bitcoin futures contracts by the CFTC and increasing acceptance of cryptocurrency exchanges by regulators have bolstered institutional adoption of Bitcoin and Ethereum. Improved regulatory clarity and oversight in many jurisdictions will further bolster institutional confidence in cryptocurrency investments.

Corporate Treasuries: Some publicly traded companies have begun allocating a portion of their treasury reserves to Bitcoin as a hedge against inflation and a long-term store of value. This trend was pioneered by companies like MicroStrategy and Tesla, which made significant investments in Bitcoin.

Digital assets high level overview and select particulars

Cryptocurrencies

Digital currencies that utilize cryptographic techniques for secure transactions and operate on blockchain networks.
Examples: Bitcoin (BTC), Ethereum (ETH), and Ripple (XRP).
Use Case: Serve as a medium of exchange, investment vehicles, or stores of value.

Stablecoins

Digital currencies pegged to stable assets, like fiat currencies, to minimize value fluctuations.
Example: USD Coin (USDC), pegged to the US dollar.

Security Tokens

Digital assets created on existing blockchain platforms, representing ownership or investment in underlying assets, often subject to regulatory requirements.
Example: Tokenized real estate or company shares.

NFTs

NFTs are unique digital tokens that signify ownership of distinct items or content, such as artwork or collectibles, on a blockchain.
Examples: CryptoPunks, Bored Ape Yacht Club.
Use Case: Facilitate the ownership and trade of unique digital items and collectibles.

Utility Token

Digital assets created on existing blockchain platforms, providing access to specific products or services within a blockchain ecosystem.
Example: Binance Coin (BNB) used for transaction fees on the Binance platform.

Digital Securities

Traditional financial securities like stocks or bonds represented digitally on blockchain platforms.
Examples: Digital shares or bonds issued through blockchain technology.
Use Case: Provide investment opportunities and increase liquidity.

Cryptocurrencies and digital infrastructure overview (1/2)

Cryptocurrencies and digital infrastructure overview

Applications can confirm the tokens in your wallet to provide users with any number of opportunities like exclusive options in games, apps that work with your token, and finance functions exclusive to cryptocurrency (e.g., DeFi).

Layer 1

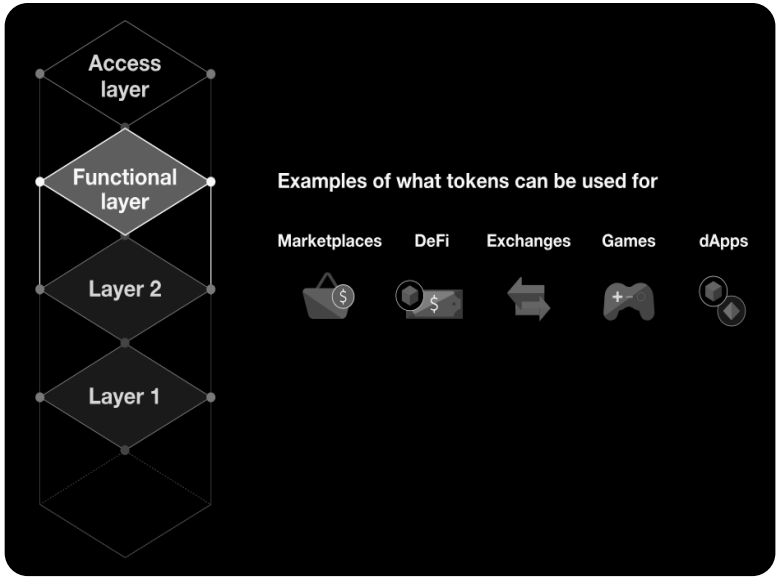
Comprises of the basic blockchain architecture that your token resides on.

Layer 2

Layer 2 scaling solutions all work differently, but their main function is to sit on top of the main chain and make transactions faster and cheaper by aggregating data.

Access layer

Includes the consumer layer interaction with this world in a visual shell.



Cryptocurrencies and digital infrastructure overview (2/2)

Cryptocurrencies and digital infrastructure overview

Applications can confirm the tokens in your wallet to provide users with any number of opportunities like exclusive options in games, apps that work with your token, and finance functions exclusive to cryptocurrency (e.g., DeFi).

Functional Layer

The top layer is made up of apps that enable users to view, trade and spend digital assets. These include:

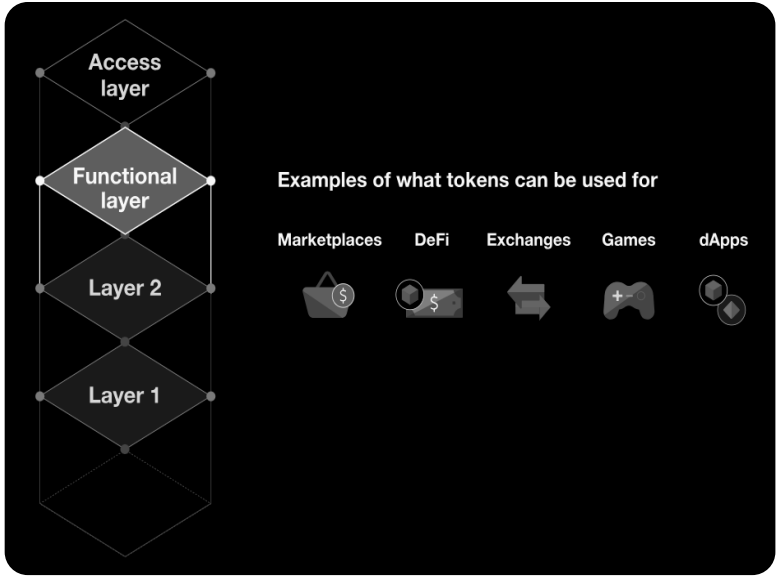
Marketplaces - comprising of digital asset products such as NFTs but may also include things beyond the blockchain ecosystem like tickets to real world experiences or the deed to a real-world asset.

DeFi - decentralized finance is an umbrella term for a variety of financial applications provided through digital assets.

Exchanges - users can trade digital assets much like in traditional FX or stock markets. Games

Games - Games built on a blockchain can offer tokenized in-game currency to their players.

dApps - Decentralized apps (dApps) includes any other applications built on a blockchain.



05

Business case studies of leading decentralized finance companies and emerging business models

Business Case Study: Aave

Aave – general overview (1/2)

Company name: Aave

- **Headquarters Regions :** London, England, United Kingdom
- **Founded Date :** 2017
- **Founders :** Stani Kulechov
- **Funding and Valuation**: $49 million

General Overview

Aave is a decentralized non-custodial liquidity protocol where users can participate as suppliers or borrowers. Suppliers provide liquidity to the market while earning interest, and borrowers can access liquidity by providing collateral that exceeds the borrowed amount.

History of Ave: A Brief Overview

Aave Protocol stands at the forefront of decentralized finance (DeFi), offering a robust platform for lending and borrowing cryptocurrencies without intermediaries. Launched in 2020 by Stani Kulechov, Aave has quickly established itself as a key player in the blockchain ecosystem. The protocol operates on Ethereum and allows users to deposit a wide range of digital assets into liquidity pools as collateral, from which they can borrow other assets at variable interest rates determined by market dynamics.

Aave pioneered the concept of flash loans, enabling instant, uncollateralized borrowing that must be repaid within a single transaction block, a feature leveraged by developers for arbitrage and complex trading strategies. Aave's governance model is decentralized, driven by its native token, AAVE, which empowers holders to propose and vote on protocol changes, ensuring community participation and adaptability. Security and transparency are paramount, with Aave employing rigorous smart contract auditing and continuous improvements to mitigate risks. Aave is a key player in providing innovative financial tools that cater to both individual users and institutional investors seeking efficient, trustless, and decentralized financial solutions.

Aave – general overview (2/2)

Founder profile

Stani Kulechov

Stani Kulechov is the Founder and CEO of Aave, an open source and non-custodial liquidity market protocol to earn interest on deposits and borrow assets. Stani was studying law at the University of Helsinki when he first started exploring how Ethereum could impact the traditional financial system. In 2017, Stani released ETHLend, one of the first DeFi DApps ever.

Vision and mission

The vision of Aave is to encourage innovation, accelerate growth, and prudently manage financial assets, while providing relevant and transparent financial reporting content. Aave is a decentralized non-custodial liquidity protocol where users can participate as depositors or borrowers. The protocol is implemented as a set of smart contracts on the Ethereum blockchain.

Business model high level overview

1 **Brief Description**

Ethereum-based P2P lending with a unique strategy that relies on collateralized loans and lending pools

2 **Lending**

Lenders must deposit funds into the network

Borrowers can access the funds and borrow

3 **Collateral**

To borrow, users must lock an amount of collateral with the value of this collateral based on USD

4 **Reserves**

Reserves are used to help the pools combat market volatility and serve as insurance to lenders when accessing liquidity pools

Aave – business model high level characteristics

Business model characteristics

Aave is a decentralized cryptocurrency platform that allows you to borrow and lend crypto, with smart contracts to automate the process.

Graph 1 - Aave Business Model

Open source	• More secure because it undergoes intense peer review from the community • Experienced investors prefer it as they can ensure all the activities and functions • There are no hidden risks or fees
Non-custodial protocol	• It never holds your cryptocurrency directly and lenders retain ownership of assets • Less risk of hacking because there are no wallets filled with users' funds to hack
Control without ownership	• Allows a borrower to gain exposure to cryptocurrencies without owning • Users earn rewards without trading digital assets which reduces the risk of loss
Rate options	• Selection of interest rate options • Offers both stable and variable interest rates to meet investment goals • Users can switch between these fee structures
Private	• Ideal for privacy-minded investors • There is no middle-man involved, no waste in filling out KYC, AML documentation
Selection	• Selection of multiple lending pools - DAI, USDC, TUSD, USDT, sUSD, BUSD, ETH, LEND, BAT, KNC, LINK, MANA, MKR, REP, SNX, wBTC and ZRX.

Aave – key features and financial products high level overview (1/2)

Key features high level overview

Aave provides a decentralized and efficient way for users to access liquidity, earn interest on their assets, and participate in the growing DeFi ecosystem.

Aave V1 also marked a crucial milestone in decentralization by transitioning administrative controls to the community through governance mechanisms, aligning with its vision of democratizing finance.

Aave V2 enhanced the protocol's risk management framework by optimizing reserve factors and parameters, increasing collateral capacity for several assets like USDC, BAT, LINK, UNI, WBTC, and WETH.

Aave V2 - Flash Loans and aTokens:

These innovations allowed users to efficiently manage and leverage assets across various decentralized finance applications. Flash Loans, particularly, revolutionized the market by enabling undercollateralized loans within a single transaction, fostering the creation of innovative financial products ("money legos") and driving substantial transaction volume.

Aave V2 - Yield and Collateral Swap:

One of the standout features is the introduction of Yield and Collateral Swap, enabling users to trade their deposited assets while they are used as collateral. This functionality reduces the risk of liquidation by allowing users to adjust their collateral positions dynamically based on market conditions. Additionally, V2 enhanced Flash Loans by integrating new functionalities like Flash Liquidations, where liquidators can use Flash Loans to efficiently execute liquidations without requiring upfront capital.

Aave V2 - Debt Tokenization:

Aave V2 introduced debt tokenization, representing debt positions as tokens that can be managed independently, facilitating native Credit Delegation. This innovation allows users to delegate credit lines to other addresses, significantly expanding access to liquidity without the need for existing capital. Gas optimizations were also a critical upgrade in V2, reducing transaction costs by up to 50% in some cases, thereby improving accessibility and scalability.

Aave – key features and financial products high level overview (2/2)

Key features high level overview

Addressing the multichain environment, Aave V3 improves user experience by supporting seamless liquidity transfers across different networks. It simplifies interactions with features like Permitlists on flashloans, which waive flash loan premiums for permitted entities, and introduces user-friendly functionalities such as repayments with aTokens instead of underlying assets.

Aave V1, V2 and V3 represent significant evolutionary steps in the Aave Protocol, each introducing new features and improvements aimed at enhancing usability, efficiency, and flexibility within the DeFi ecosystem.

Aave V3 - portal and high efficiency mode (E-Mode)

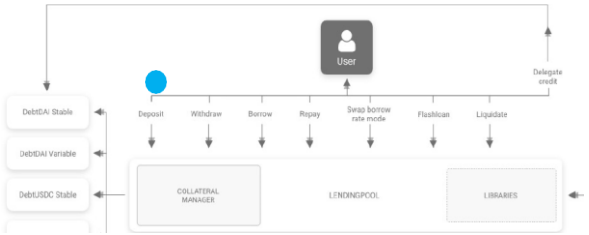
These innovations Aave V3, enhances capital efficiency by introducing innovative features like Portal and High Efficiency Mode (E-Mode). Portal facilitates seamless asset movement across different Aave markets on various networks, leveraging aTokens' pegged design to optimize liquidity utilization. E-Mode categorizes assets based on risk parameters, allowing borrowers to maximize their borrowing power within specific asset categories. This approach not only increases efficiency but also enables new use cases such as efficient yield farming and diversified risk management.

Enhanced risk management in Aave V3 includes Supply and Borrow Caps configured by Aave governance to mitigate risks like infinite minting and oracle manipulation. Granular borrowing power control allows governance to adjust asset exposure without impacting existing borrowers, thereby bolstering protocol resilience against market volatility and asset fluctuations.

Aave V3 continues to prioritize decentralization with improvements in asset listing strategies. It introduces Asset Listing Admins, enabling alternative asset listing methods beyond on-chain voting. This flexibility fosters a more dynamic and responsive protocol governance, accommodating a broader range of asset types and use cases while maintaining security and decentralization principles.

Aave – an overview of the lending pool process and mechanism

The Lending Pool Mechanism



The Lending Pool Process

Process Maps

- Deposit
- Borrow
- Repay
- Swap
- Liq. Call

Lending pool high level overview

The central mechanism that allows Aave to function is that deposits go into something called a “liquidity pool” which the protocol can then use to make loans to others.

Steps to access the lending pool using Aave:

Deposit: Deposit a certain amount of an asset into the protocol, minting the same.

amount of corresponding aTokens and transferring them to the caller’s address.

Withdraw: Withdraw the amount of the underlying asset, i.e. redeems the underlying token and burns the aTokens.

Borrow: The borrow action transfers to the user a specific amount of underlying asset, in exchange of a collateral that remains locked.

Repay: The repay action allows the user to repay completely or partially the debt.

Swap borrow rate mode: Allows a user to swap between variable and stable rate.

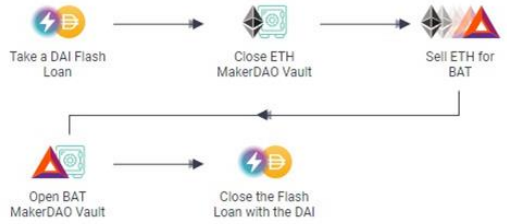
Flash loans: The flash loan action will allow users to borrow from the reserves within a single transaction, as long as the user returns more liquidity that has been taken.

Liquidation call: When the health factor of a position is below 1, liquidators repay part or all of the outstanding borrowed amount on behalf of the borrower, while receiving a discounted amount of collateral in return.

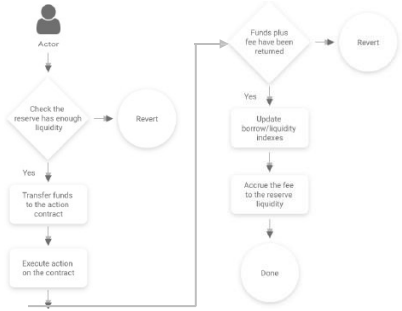
Delegate credit: Through the concept of delegation, users can delegate to other addresses by opening a credit line.

Aave – an overview of the flash loans process and mechanism

Flash Loans Mechanism



Flash Loans Process



Flash loans high level overview

A flash loan is an instant loan with one condition — it must be repaid within a single Ethereum transaction. There are several Ethereum-related basics to consider to better understand how the process works.

An Aave flash loan can be thought of in three simple steps:

i) A user borrows tokens from one of Aave's lending pools

ii) The parameters for the loan are executed on the Ethereum blockchain.

iii) The user must repay the borrowed amount plus Aave's loan service fee within the same transaction.

If the last condition is met, then the entire transaction goes through and is immutably added to Ethereum's ledger. If the last condition is not met, then the entire transaction is rejected, and all network commands are voided as if no transaction occurred.

Flash loans use case

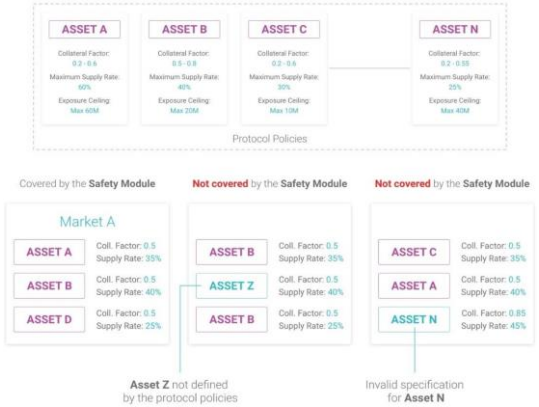
The most common use cases involve collateral-based loans.

Example: If users borrow DAI while using ETH as collateral and the price of ETH was crashing, the borrower would be in danger of having their loan liquidated. In this situation, the borrower could use a Flash Loan to swap their volatile ETH asset for a stablecoin. The user's collateral value would now be stable, and you would avoid all the penalties that come with being liquidated.

Aave – protocol governance model (1/2)

Governance Process

Governance Policies



Governance high level overview

Aave is a fully decentralized, community governed protocol by the AAVE token-holders. AAVE token-holders collectively discuss, propose, and vote on upgrades to the protocol. AAVE token-holders (Ethereum network only) can either vote themselves on new proposals or delegate to an address of choice.

Key particulars of the governance process:

- ✓ Decision-making process for the different risk parameter changes, improvements and incentives
- ✓ Future decisions governing the protocol will be enacted through governance procedure
- ✓ The AAVE token empowers holders with the capability to vote on proposals and collectively act as governors of the protocol

Governance structure and components

Protocol policies govern the overall behavior of the protocol and the entities belonging to it. They regulate specific aspects of the protocol related to safety, economics and expansion.

Market policies are defined in the context of each market and, for markets belonging to the Aave ecosystem, they are specified within the boundaries identified by the Protocol Policies. A market participating in the Aave ecosystem needs to operate under safety policies that are not violating the protocol safety policies.

Aave – protocol governance model (1/2)

Protocol policies particulars

A. Risk Policies

The Risk Policies define the set of rules that ensure the safety and protection of the protocol and the users participating in it. Risk Policies include, but are not limited to, decision-making for:

Assets compatible for integration within Aave:

i. The list of assets for which risk is deemed acceptable for the safety of the protocol.

Modelling of the interest rates:

i. Interest rates modelling is a key risk parameter as it determines the actual yield for depositors, the ratio between borrowed, available liquidity and the general the competitiveness of a market for a specific asset.

Base risk parameters for overcollateralization and liquidation:

i. The risk parameters that are governed by AAVE affect all money markets and set global boundaries for those markets.

Configuration and behavior of the Safety Module (SM):

i. The Safety Module is one of the core components of the Aave Ecosystem which is regulated by a set of rules and behaviors.

Acceptance of new money markets:

i. Anyone will be able to instantiate their own money market within the Aave Protocol subject to approvals.

B. Improvement Policies

Improvement policies define rules under which ecosystem improvements are incepted, developed and applied to the ecosystem, including but not limited to i) smart contracts ii) safety module iii) governance processes iv) AAVE token contract v) governance contracts.

C. Incentive Policies

Incentives Policies define the rules under which token incentives in Aave are generated.

Incentives are used to shape behaviors within the ecosystem to achieve a common objective.

For Aave, the common goal is to ensure the safety of the Aave Protocol, cost-efficient usage by the market participants, and proper ecosystem incentives to drive innovation and long-term growth of the ecosystem.

D. Safety Incentives

Safety Incentives ensure the safety of the protocol by incentivizing AAVE holders to participate.

This is achieved with a set of incentives pushing behavior to naturally create a positive feedback loop within the Protocol. In that sense, the essence of those systemic incentives is to materially fade away while having lasting impact on participants behavior.

Aave – protocol governance model (2/2)

Market policies particulars

Market Policies

The Aave Protocol will eventually allow anyone to create a money market. However, to benefit from protocol incentives, the market parameters and assets selected must be within the realm of the Risk Policies.

The following list describes which parameters must be defined at inception by market creators :

Supported assets select functionality:

i) provide liquidity and borrow from while the currency should be validated by the higher layer protocol governance.

ii) use as collateral while the currency should be already validated by the higher layer protocol governance.

Enable / disable borrowing modes of an asset: variable, stable or any other mode included in the future of the protocol.

Market-specific components: smart contract updates for new versions already approved by the Protocol Governance or the addition of smart contract modules, optional per market.

Risk configurations per asset: loan-to-value, liquidation threshold, liquidation bonus and automatic liquidation parameters.

Interest rates model per asset: adjustment of the curves which determine the relationship between the state of each asset's reserve and its interest rates.

Aave – Key investors and funding rounds

Key Investors and Funding Rounds

The Aave project raised funds through several private sales and an initial token auction, securing investments from major venture capital firms and institutional investors. It has a total funding amount of $49M across 3 rounds with 20 investors. Here are some of the investors:

- **Seed Rounds:** Crowd Venture Capital, Google, IBM, Samsung Electronics, Cashican People, Buck Stash, CoinD
- **Initial Coin Offering:** DTC Capital, ParaFi Capital, Framework Ventures, Ganesh Kompella
- **Secondary Markets:** Iconium and other angel investors
- **Venture Round:** Standard Crypto, Blockchain.com Ventures, Genesis One Capital

Business Case Study: Uniswap

Uniswap – general overview (1/2)

Company name: Uniswap

- **Headquarters Regions :** New York, United States
- **Founded Date :** November 2, 2018
- **Founders :** Hayden Adams
- **Funding and Valuation:** Valuation of $1.6B after series B of $165M

General Overview

Uniswap is a decentralized exchange (DEX) built on the Ethereum blockchain, utilizing an Automated Market Maker (AMM) model. The model ensures constant liquidity and reduces the reliance on a centralized entity to match buyers and sellers. Users can become Liquidity Providers by creating pools of two tokens. In return they receive fees generated from trade on that pool, proportional to their contribution in the pool.

History of Uniswap: A Brief Overview

Founded by Hayden Adams, Uniswap has become one of the most prominent and influential DeFi protocols in the cryptocurrency ecosystem. Launched in November 2018, Uniswap V1 marked a pioneering advancement in decentralized finance (DeFi) by introducing the concept of automated market makers (AMMs) to Ethereum-based decentralized exchanges. At its core, Uniswap V1 operated using constant product pools, where liquidity providers (LPs) deposited equal values of two ERC-20 tokens, establishing an automated pricing mechanism without the need for order books. This innovation simplified token swapping for users, who could trade ERC-20 tokens directly through a straightforward interface, relying on smart contracts to execute trades and maintain liquidity. LPs earned fees proportional to their share of the pool's liquidity, based on the volume of trades.

However, Uniswap V1 had limitations compared to subsequent versions, such as the absence of features like price oracles and the inability to support complex trading strategies or concentrated liquidity positions. Despite these limitations, Uniswap V1 laid the groundwork for decentralized exchanges and popularized the AMM model, influencing the development of subsequent iterations like Uniswap V2 and V3, which aimed to enhance functionality, efficiency, and flexibility in decentralized trading protocols.

Uniswap – general overview (2/2)

Founder profile

Hayden Adams

Graduated from Stony Brook University with a degree in Mechanical Engineering, Hayden Adams worked as an engineer at Siemens. Inspired by Vitalik Buterin and Ethereum, Hayden aimed to create a decentralized crypto exchanged with automated market maker. After launching Uniswap in 2018, Hayden received funding from Ethereum, Paradigm, a16z, etc.

Vision and mission

Uniswap's vision is to revolutionize the trading experience by offering a decentralized platform in contrast to the traditional platforms. This more transparent environment addresses the previous shortcomings such as security risks and liquidity issues. With the pioneering AMM, Uniswap provides users with lower fees and trustless trading options, allowing them to earn rewards and participate in governance through the native ERC-20 token, UNI, which ensures a community driven approach to DeFi.

Business model high level overview

1 **Brief Description**

Decentralized trading protocol on Ethereum, utilizing an AMM system to enable continuous liquidity without order books.

2 **Trading**

Users engage in token swaps using liquidity pools, facilitated by smart contracts that automate execution and ensure fair pricing.

3 **Liquidity Pools**

To trade, users provide liquidity by depositing pairs of tokens, earning fees proportional to their stake in the pool.

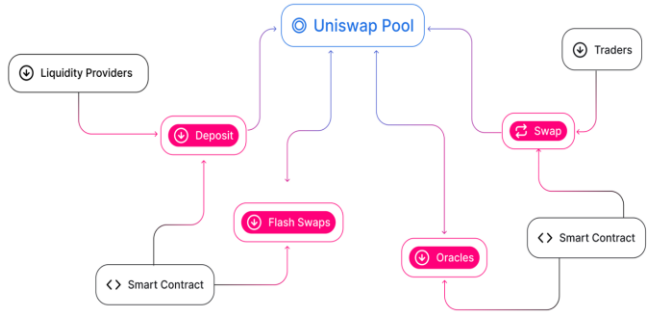
4 **Reserves**

Uniswap uses a portion of transaction fees to bolster pool reserves, enhancing the platform's financial stability against market volatility.

Uniswap – business model high level characteristics

Business model characteristics

Uniswap Ecosystem



In the Uniswap ecosystem, liquidity providers deposit assets into pools and receive transaction fees based on their stake in return these pools are managed by smart contracts that automate the trading process, allowing traders to swap tokens. Uniswap also facilitates advanced trading strategies through features like flash swaps, which enable immediate token exchanges without upfront capital, and integrates oracles for accurate pricing data.

Open source	• As an open-source protocol, Uniswap invites contributions and enhancements from the community, fostering continual development and adaptation • Transparent operations ensure all protocol actions are verifiable
Decentralization	• Permissionless trading allows users to trade cryptocurrencies directly from their wallets without intermediaries • Decentralized governance model uses UNI governance tokens to involve the community in decision-making
Automated Market Making	• With a constant product formula, the model adjusts prices based on supply and demand dynamics, ensuring liquidity and minimizing slippage. • Users are encouraged to deposit assets into liquidity pools to earn fees proportional to their contribution.
Revenue Streams	• Uniswap's revenue is derived from a combination of trading fees, liquidity provision rewards, protocol fees allocated by governance decisions, and the potential appreciation of its governance token.

Uniswap – key features and development roadmap (1/2)

Uniswap V1

Launched in November 2018 at Devcon 4, this is the inaugural version of this decentralized trading protocol. It's designed with a focus on simplicity, decentralization, and security, facilitating the seamless exchange of ERC20 tokens on the Ethereum blockchain.

Key features of Uniswap V1 include support for any ERC20 token through the Uniswap factory, which allows users to add liquidity to ETH-ERC20 pairs and collect transaction fees. The protocol uses a liquidity-sensitive automated pricing model based on the constant product formula, enabling straightforward token swaps—including ETH to ERC20 conversions without the need for wrapping and direct ERC20 to ERC20 transactions in a single step.

Other features include the creation of private and custom exchanges that allow users to tailor liquidity pools to specific needs and strategies such as fund management or alternate pricing mechanisms. In addition, V1 facilitates the purchase of ERC20 tokens using the Ethereum Name Service (ENS), enhancing the accessibility and ease of transactions. Moreover, the platform maintains the lowest gas fees among all decentralized exchanges, with transfers to multiple addresses in a single transaction allowed. These features collectively set a strong foundation that invite continuous growth and innovation within the ecosystem.

Uniswap V4

Uniswap V2 was launched in May 2020, maintaining the fundamental AMM while introducing several pivotal enhancements. Unlike V1, which required ETH as a bridge currency in every trading pair, V2 permits the creation of arbitrary ERC20/ERC20 pairs in addition to ETH-based pairs, broadening trading options and reducing dependence on ETH. Moreover, V2 introduces "flash swaps," allowing users to temporarily utilize assets across Ethereum contracts without upfront costs, settling the assets' value only upon transaction completion.

V1 is considered insecure for use as an on-chain price oracle due to its susceptibility to manipulation. For instance, if a derivative contract relies on the current ETH-DAI price from V1 to settle trades, an attacker could exploit this by buying ETH at an inflated price, thereby misleading the derivative contract into settling at a higher value. The attacker could then sell ETH back to the exchange at the true price, potentially executing this as a single transaction or with the assistance of a miner controlling transaction order within a block. V2 addresses this issue with by recording the price at the beginning of each block or after the last transaction of the previous block. It accumulates these prices by tracking the cumulative sum at the start of each block, with each price weighted based on the time elapsed since the last block update. This approach ensures that the oracle's cumulative value accurately reflects the sum of spot prices over time, enhancing reliability and resistance to manipulation.

Uniswap – key features and development roadmap (2/2)

Uniswap V3

Uniswap V3 was launched in May 2021 with a focus on capital efficiency and optimizing liquidity provision. Earlier versions were designed to provide liquidity across the entire price spectrum from 0 to infinity, often resulting in large portions of assets in a pool remaining untouched. In response to this inefficiency, V3 introduced a new concept allowing LPs to concentrate their assets within specific price ranges rather than the entire spectrum, allowing them only needing to maintain reserves that support trading within that specific range. Within each position, V3 operates similarly to a constant product pool, but with larger virtual reserves tailored to the price range. LPs in V3 have the flexibility to create multiple positions, each focused on a specific price range. This means they can strategically allocate liquidity across different parts of the price spectrum according to market demand and their own risk preferences. For instance, LPs can concentrate their assets in narrower price bands around the current market price, with the option to adjust their positions by adding or removing tokens as prices fluctuate.

V3 also adjusts the fee structure. Previously, each pair of tokens had only one liquidity pool with a fixed fee of 0.30% for all trades–too high for stablecoin pairs and possibly too low for pools involving highly volatile or less frequently traded tokens. V3 changes this by allowing multiple liquidity pools for each token pair, each with a different swap fee. These pools can have fees set at 0.05%, 0.30%, or 1% initially, with the possibility of additional fee tiers being added through governance decisions by UNI token holders.

Uniswap V4

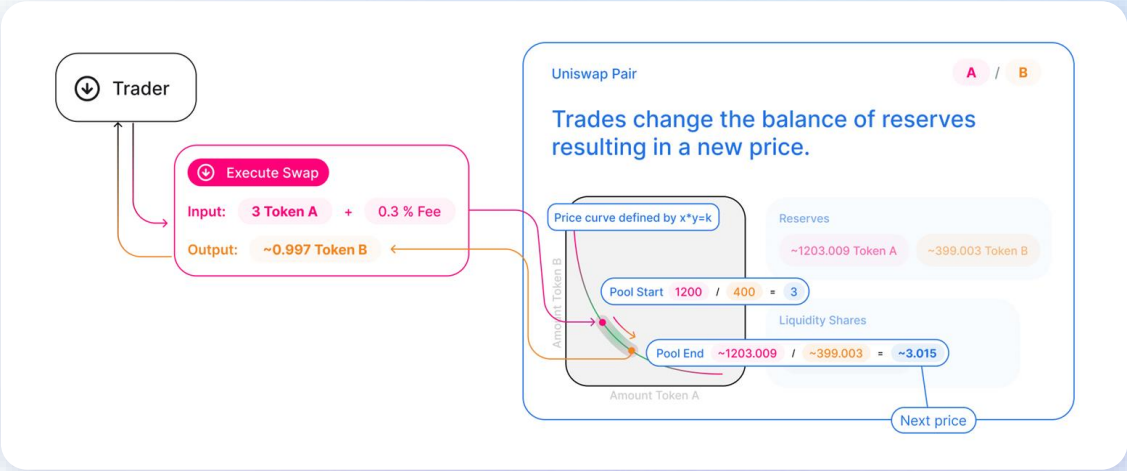
Uniswap V4 is currently under development to enhance how liquidity is provided and how tokens are traded. A pivotal feature in V4 is the introduction of "hooks", a feature that allows for customization of liquidity pools. These hooks enable developers to embed specific functionalities into the pools at critical points of their operational life cycle. This level of customization could range from altering order types, oracles, and AMM curves to integrating unique fee models, thereby allowing for a tailored approach that meets diverse market demands and trading strategies.

V4 introduces an architectural improvement with the Singleton contract, which consolidates all liquidity pools into one contract. This change drastically reduces the gas costs associated with trading and creating pools, making multi-hop trades more efficient since tokens don't need to be transferred between multiple contracts. The cost of creating a new pool in V4 is 99% lower than in V3, making it much more accessible to set up new pools. The new "flash accounting" system also enhances transaction efficiency by enabling users to combine multiple actions—like swapping tokens and adding liquidity—into a single transaction. It monitors the net token balances throughout the transaction, and if any discrepancies arise and debts are not settled by the transaction's close, it automatically reverts to prevent any losses or errors.

Uniswap – an overview of the trading mechanism

The liquidity pool and underlying formula

By using an automated liquidity protocol consists of pairs of ERC-20 tokens, Uniswap eliminates the need for traditional market makers. These pools operate under a mathematical principle known as the constant product formula, ensuring liquidity and enabling continuous trading without the need for external interventions or traditional order books. Anyone can become an LP by depositing an equivalent value of each token in a pair. In return, LPs receive pool tokens that represent their share of the total reserves in the pool.



The backbone of Uniswap's AMM system is the constant product formula, mathematically expressed as XY=K. Here, X and Y represent the reserves of two different tokens in a liquidity pool, and K is a constant that remains stable through every trade. This formula ensures that the product of the reserves cannot change, thereby preserving the pool's overall liquidity. For instance, the liquidity pool starts with 1200 units of Token A and 400 units of Token B, establishing an initial price ratio of 3 Token A for each Token B. When a trader executes a swap to trade 3 units of Token A for Token B, the formula adjusts the reserves to maintain the constant K. The trade introduces a 0.3% fee, factored into the transaction. Post-trade, new reserves looks like 1203.009 Token A and 399.003 Token B with a new price ratio of 3.015 between the two tokens, indicating a slight increase in the price of Token B relative to Token A that is reflected by a downward movement along the price curve.

Uniswap – an overview of flash swaps and applications

Flash swaps mechanism allows users to withdraw the reserves of any ERC-20 token on Uniswap without requiring upfront capital. Hence users have the options to perform complex multi-step transactions and either repay the withdrawn tokens with the corresponding pair tokens by the end of the transaction. This is facilitated by a swap function that includes a callback to a user-defined contract, enabling actions between transferring out requested tokens and verifying the trade's invariant. After the callback finishes, Uniswap checks the updated balances to ensure they meet the invariant, adjusting for any fees paid. If the contract lacks sufficient funds, the entire transaction is reverted for security. Additionally, users can repay Uniswap using the same token received from the swap, essentially allowing anyone to temporarily borrow assets from a Uniswap pool, subject to a 0.30% fee similar to the trading fee charged by Uniswap.

Here are two applications of flash swaps:

- **Capital-Free Arbitrage**: Traditionally, arbitrage opportunities are limited to those with sufficient capital to act quickly on price discrepancies between different markets. With the introduction of flash swap, users can leverage Uniswap's liquidity without initial funds, significantly democratizing access to arbitrage. For example, if ETH is priced at 200 DAI on Uniswap but sells for 220 DAI on another exchange, a user can utilize a flash swap to withdraw ETH from Uniswap, sell it for DAI on the external platform, and repay Uniswap while retaining the profit, all within a single transaction.
- **Instant Leverage**: Flash swaps enhance leverage strategies. In a scenario where a user wants to leverage ETH holdings in conjunction with a lending protocol, this would typically involve multiple transactions and gas fees to deposit ETH, mint DAI, and exchange DAI for more ETH. However, with flash swaps, the user can withdraw the desired amount of ETH upfront, deposit it into the protocol to mint the maximum allowable DAI, repay the swap, and retain the leveraged position in a single transaction. This offers users a more efficient way to manage leveraged positions and significantly reduces transaction complexity and costs.

Uniswap – protocol governance model (1/3)

Governance process

Governance high level overview

Uniswap's governance model is a structured process that enables community-driven decision-making for the protocol, aligning with the principles of DeFi. This model empowers UNI token holders to propose, discuss, and vote on significant changes to the platform, such as protocol upgrades, parameter adjustments, and fund allocations. .

Step-By-Step Governance Process

Phase 1: Temperature Check – To gauge initial community interest in a proposed change

- A proposal is posted on the discussion forum (gov.uniswap.org) with a non-biased question regarding a potential change.
- A corresponding poll on Snapshot allows users to vote to signal their support or opposition.
- The poll remains open for three days, and a minimum of 25,000 UNI in favor is needed to advance the proposal.

Phase 2: Consensus Check – To refine the proposal with community feedback and establish support

- A new poll is created on Snapshot, incorporating feedback from the Temperature Check phase.
- The proposal is discussed further on the forum, and participants are encouraged to share their thoughts and build support.
- The poll is open for five days, requiring a minimum of 50,000 UNI for the proposal to pass this stage.

Phase 3: Governance Proposal – To finalize and vote on the proposal for official implementation

- A formal proposal is drafted with required code changes and submitted through a governance portal.
- The proposal must be supported by at least 10 million UNI to be eligible for voting.
- A seven-day voting period follows, during which the community votes on the proposal. If it passes, a two-day timelock is triggered before the changes are executed.

Uniswap – protocol governance model (2/3)

Glossary of Key Terms

UNI

UNI is an ERC-20 token that determines a user's influence within Uniswap's governance system. The more UNI tokens a user holds, the greater their voting power.

Delegation

UNI holders must delegate their voting rights to a specific address to participate in voting or to create proposals. Delegation can be assigned to any address, including the holder's own, and does not lock the tokens.

Proposal

This is a formal request to modify the protocol or treasury. Proposals involve executable code and must be supported by at least 0.25% (2.5 million UNI) of the total UNI supply to be eligible for submission. Once submitted, proposals undergo a seven-day voting period. If a proposal's required vote weight falls below the necessary threshold during this time, it can be canceled by any community member.

Quorum

For a proposal to be approved, it must meet a quorum of 4% of the total UNI supply (40 million UNI) voting in favor.

Timelock

Timelock contract ensures that any governance actions in Uniswap are implemented with a mandatory delay of 2 days. For major updates, the delay can extend up to 30 days.

Protocol Token – UNI

Key Features

The UNI token is an essential component of Uniswap's governance framework. It embodies the ethos of decentralization, granting voting rights to all token holders and enabling them to have a direct impact on the governance and development of the Uniswap protocol. By distributing UNI tokens to users and liquidity providers, Uniswap aligns incentives across its ecosystem.

Distribution and Tokenomics

Total Supply: 1 billion UNI tokens were minted at the genesis and will be distributed over a period of four years.

Allocation Breakdown:

- 60.00% (600 million UNI) allocated to Uniswap community members, with 15% of this already distributed to past users.
- 21.266% (212.66 million UNI) reserved for team members and future employees, subject to a four-year vesting schedule.
- 18.044% (180.44 million UNI) allocated to investors, also with a four-year vesting period.
- 0.69% (6.9 million UNI) set aside for advisors, with the same four-year vesting condition.

Inflation Rate: After the initial four-year distribution period, UNI will have a perpetual inflation rate of 2% per year to encourage continued participation and discourage passive holding.

Uniswap – protocol governance model (3/3)

Potential Adversarial Challenges

Scenario 1: Exploitable Proposals and Vote Manipulation

A scenario could occur where a proposal, initially brought forward with good intentions, is discovered to have a vulnerability. A malicious actor could then leverage this weakness by quickly acquiring enough UNI tokens to sway the vote in their favor and exploit the proposal once it passes. To mitigate this, Uniswap currently requires that voting power be delegated before or immediately after a proposal is submitted, leaving little time for such manipulative tactics. However, increasing the proposal delay could introduce new risks, as it might allow more time for malicious activities to be planned.

Scenario 2: Market Manipulation and Collusion

Another risk involves bad actors colluding to force through a harmful proposal by manipulating the UNI market. By accumulating a significant amount of UNI, these actors could pass a proposal that serves their interests but harms the community. While executing such a strategy would be costly and difficult, given the need for at least 40 million UNI to achieve a quorum, it remains a theoretical risk. In the event of such a takeover, the Timelock mechanism would provide a critical buffer to allow community members to react and potentially fork the protocol to maintain its integrity.

Scenario 3: Flash Loan Attacks

Flash loans pose a unique threat to governance processes, as they allow users to borrow large sums of UNI temporarily without collateral. This could be exploited to push through proposals or spam the governance system, disrupting its normal function. Uniswap's governance requires that any proposal submitter maintain a minimum balance of 2.5 million UNI throughout the voting period, preventing flash loan abuses that span multiple blocks and ensuring that governance decisions are made by committed stakeholders.

Scenario 4: Incentivized Bad Faith Voting

There is also the possibility of a proposal that incentivizes bad faith voting, such as offering rewards to those who vote in favor of draining the treasury while penalizing those who vote against. While Uniswap's governance framework does not have a direct mechanism to prevent such proposals, market dynamics provide a natural deterrent. The market value of UNI would likely plummet in response to any such malicious proposal, reducing the attractiveness of the attack and dissuading participation in bad faith voting.

Uniswap – Key investors and funding rounds

Key Investors and Funding Rounds

Uniswap has raised a total of $176M in funding over 3 rounds, with the latest funding raised on Oct 13, 2022, from a Series B round.
Here are some of the investors:

- **Seed**: Coinbase, Blockchain Fund Chelyabinsk, Version One Ventures, Blockchain Capital, Maven 11 Capital, Ribbit Capital, Skycatcher
- **Series A:** Version One Ventures, Paradigm, ParaFi Capital, SV Angel, Variant Alternative Income Fund, A.Capital Ventures, Union Square Ventures, Andreessen Horowitz
- **Series B**: a16z crypto, SV Angel, Variant, Paradigm, Polychain

LIDO

Business Case Study: Lido Finance

Lido – general overview (1/2)

Company name: Lido

- **Headquarters Regions :** George Town, Cayman Island
- **Founded Date :** October 2020
- **Founders :** Vasiliy Shapovalov, Konstantin Lomashuk
- **Funding and Valuation:** Market cap of $0.95B with 5 founding rounds of $167M in total

General Overview

Lido provides a liquid staking service for Ethereum, enabling users to earn staking rewards without locking their assets or managing staking infrastructure. The DAO controls the deposited funds, and node operators selected by the DAO stake the tokens without having direct access to the users' assets. Lido offers a flexible staking solution, eliminating the need for maintaining validator nodes and allowing users to stake any amount of ether without restrictions.

History of Lido: A Brief Overview

Founded by Jordan Fish, Vasiliy Shapovalov, and Konstantin Lomashuk, Lido emerged as a solution to the limitations of early staking mechanisms on Ethereum's Beacon Chain. Launched in December 2020, Lido introduced liquid staking, allowing users to stake tokens without locking them up or maintaining staking infrastructure, and receiving stETH tokens that could be freely traded or used within DeFi applications. This innovation opened up staking to a broader audience, eliminating barriers like illiquidity and high minimum staking requirements.

Over the years, Lido expanded its support beyond Ethereum to include networks like Polygon, Solana, and others, although some, like Terra and Polkadot, were later discontinued. Key milestones include the launch of the wstETH token, bridging to various blockchains, and the deployment of the Simple DVT module to further decentralize node operations. With each update, Lido has continued to refine its offerings, demonstrating a commitment to enhancing accessibility and decentralization in staking across the crypto ecosystem.

Lido – general overview (2/2)

Founder profile

Vasiliy Shapovalov

Co-founder of Lido and the tech lead for stETH. With over a decade of experience in software development, Vasiliy also serves as the CTO of P2P Validator.

Konstantin Lomashuk

Co-founder of Lido, and the founder of P2P Validator. He also co-founded Cyber Fund and holds a PhD in finance from Kaliningrad State Technical University.

Vision and mission

Lido's vision is to simplify and democratize staking by offering a liquid staking solution that removes traditional barriers. This approach enables users to earn staking rewards while freely using their staked assets in various DeFi applications, such as lending, trading, and yield farming. By supporting multiple PoS networks and maintaining decentralization through its DAO governance model, Lido aims to create a more inclusive and resilient staking ecosystem.

Business model high level overview

1 **Brief Description**

Lido offers a liquid staking solution for Proof-of-Stake networks, allowing users to stake tokens without locking them.

2 **Node Management**

A network of node operators manages the staking process, selected by the Lido DAO to ensure security and decentralization.

3 **Liquid Staking**

Users receive liquid tokens (e.g., stETH) when they stake, which can be used in DeFi applications while earning staking rewards.

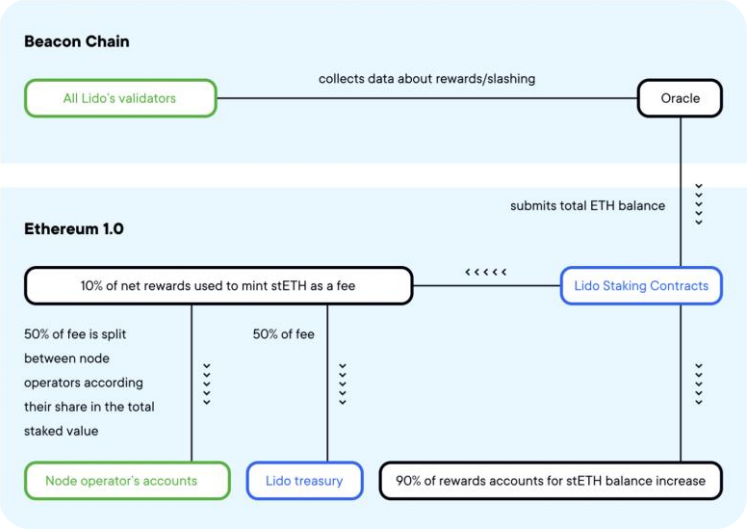
4 **Governance**

The Lido DAO, governed by LDO token holders, makes decisions on protocol upgrades, fees, and node operator selection.

Lido – business model high level characteristics

Business model characteristics

Lido Business Model



Lido's business model revolves around its innovative liquid staking mechanism, which simplifies the staking process and provides continuous liquidity for staked assets.

1. **Staking ETH**: When users stake ETH through Lido, they deposit their tokens into Lido's staking contracts and receive stETH tokens in return.
2. **Reward Generation**: The staked ETH is delegated to Lido's network of validators, who participate in the Ethereum network's proof-of-stake consensus mechanism. Validators earn rewards from transaction fees, MEV (maximal extractable value), tips, and protocol inflation, which are collected and aggregated by Lido.
3. **Fee Distribution**: Lido takes a 10% cut from the total staking rewards as a service fee. This fee is divided into two parts:
    a. Node Operators: 50% of the collected fee is distributed among the node operators according to their share of the total staked value.
    b. Lido Treasury: The other 50% is allocated to the Lido DAO treasury. These funds are used for protocol development, maintenance, and community initiatives.
4. **Reward Allocation to stETH Holders**: The remaining 90% of the staking rewards are reinvested back into the stETH token supply, effectively increasing each stETH holder's balance proportionally to their holdings.

Lido – key features and development roadmap (1/2)

Technological Highlights of Lido's Platform

Introduction of Liquid Staking Derivatives

Lido's primary innovation is its liquid staking derivative tokens, such as stETH, allowing users to stake assets without locking them up.

Cross-Chain Integration and Compatibility

Lido has developed bridges for its staking tokens across multiple blockchain networks. This includes integration with platforms such as Arbitrum, Optimism, BNB Smart Chain, and Avalanche, enhancing cross-chain liquidity.

Distributed Validator Technology (DVT)

One of Lido's significant technological advancements is the adoption of Distributed Validator Technology (DVT). This technology groups validators into independent committees, which work together to propose and attest to blocks, reducing the risk associated with individual validator failures. By splitting the validator's signing keys across several nodes, DVT enhances the protocol's resilience and security.

Staking Router and Dynamic Node Management

The staking router is a sophisticated smart contract that enhances the efficiency of stake distribution across Lido's node operators. It dynamically allocates staked assets to validators based on specific criteria, such as performance and capacity. This system allows for automatic adjustments in real-time, responding to network conditions and validator status.

Permissionless Staking and Community Involvement

Lido is implementing permissionless staking modules that use smart contracts to automate the onboarding process for new validators. These modules allow anyone to join the validator set without requiring manual approval, streamlining network expansion.

Dual Governance Mechanism

Lido's dual governance mechanism adds a layer of security and control by allowing stETH holders to lock their tokens in a veto-signaling escrow contract. This contract monitors the amount of locked tokens, and if a set threshold is reached, pauses any proposed protocol changes, providing a safeguard against rapid or contentious modifications.

Lido – key features and development roadmap (2/2)

Lido on L2: Embracing Dencun for Greater Scalability

Adapting to Ethereum's Decun Upgrade

With the upcoming Ethereum Dencun hardfork and the introduction of EIP-4844, Lido is positioning itself to expand its presence and functionality on Layer 2 (L2) networks. EIP-4844 introduces Proto-Danksharding to Ethereum, enabling significant fee reductions for L2 rollups by incorporating blob transactions into blocks. This change is part of Ethereum's "The Surge" phase, aimed at enhancing scalability and reducing transaction costs across the network.

Expanding wstETH Across Layer 2 Networks

Lido has been actively expanding its wrapped stETH (wstETH) across multiple L2 networks, including Arbitrum, Optimism, Polygon, and more, facilitating broader access to staking rewards and opportunities. The Lido Network Expansion Workgroup has focused on ensuring security and risk isolation in this process by leveraging canonical bridges and segregating tokens across distinct bridge contracts. This approach minimizes cross-domain risks and aligns with Ethereum's rollup-centric roadmap.

Innovative Bridging Architecture

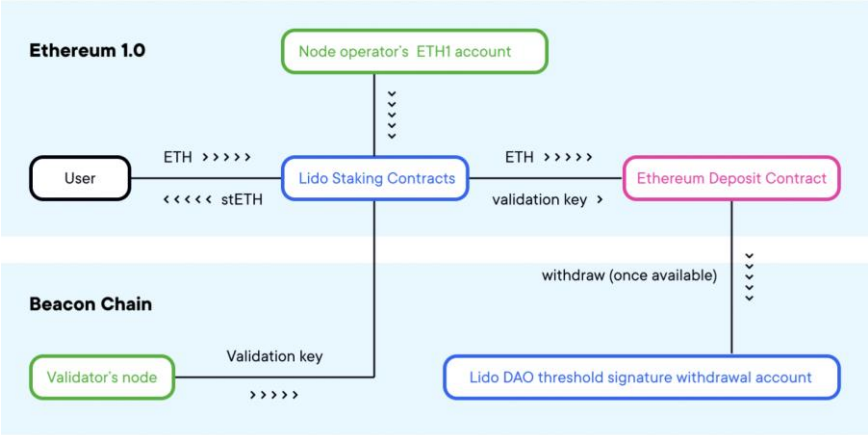
The proposed bridging architecture involves deploying dedicated bridge contracts on both L1 and L2, governed by Lido DAO. This design supports various functionalities including the capability to pass arbitrary data, revamp token logic, and pause or resume bridging in emergencies. The architecture also prepares for future updates by enabling integration with new token standards.

Future Developments for Rebaseable stETH on Layer 2

Looking ahead, Lido aims to further develop its support for rebaseable stETH across L2 networks. This includes potential features like facilitating staking and withdrawal requests directly from L2, allowing gas payments in stETH, and supporting cross-domain deposits and withdrawals.

Lido – an overview of the staking mechanism (1/2)

Lido's Staking Process and Flow of ETH



Lido's staking mechanism is built around a robust set of smart contracts that manage the entire staking process for Ethereum and other supported proof-of-stake blockchains. At its core is the Staking Pool, a contract that handles the deposit and withdrawal of ether (ETH), the minting and burning of stETH tokens (Lido's liquid staking token), and the distribution of funds to node operators.

Staking with Lido and stETH Tokens

To stake with Lido, users send their ether to a smart contract and receive stETH tokens in return. These stETH tokens represent the staked deposit and can be held, traded, or sold. The balance of stETH is determined by the total amount of staked ether, including staking rewards, and adjusted for any slashing penalties incurred by validators. Deposits into Lido are allocated to node operators who validate using these deposits. However, node operators do not have direct access to the users' ether. The ether is deposited into the Lido protocol's smart contract and subsequently locked into Ethereum's proof-of-stake deposit contract. A threshold signature account controlled by the Lido DAO is specified as the withdrawal address for staking. Withdrawals of staked ether will only be possible once Ethereum 2.0 implements transfers and smart contracts.

Lido – an overview of the staking mechanism (2/2)

Introduction to wstETH

After receiving stETH tokens in return for staking ether with Lido, users have the option to "wrap" these tokens into wstETH. This wrapped version of stETH is specifically designed for seamless integration with DeFi platforms. Unlike stETH, which has a balance that fluctuates daily due to staking rewards, wstETH maintains a fixed balance while using an underlying share system to reflect staking rewards. This fixed balance is crucial for compatibility with many DeFi protocols, such as Uniswap and MakerDao, that require a constant balance mechanism. By converting stETH into wstETH, users can ensure that their assets remain productive across various DeFi platforms while continuing to benefit from the staking rewards accrued by their underlying stETH.

Node Operators and Capital Efficiency

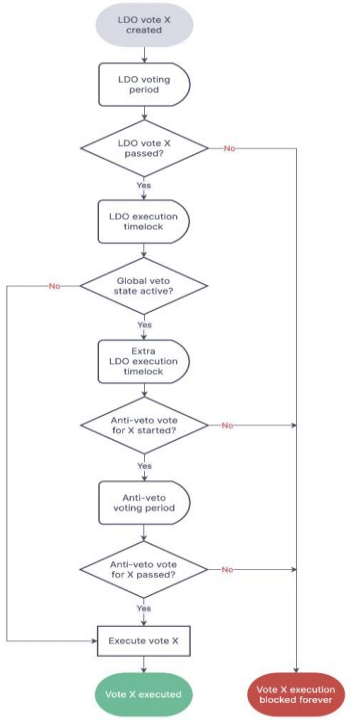
Lido's system does not require node operators to provide equal collateral for their staking positions. Instead, node operators are selected based on their track record in asset staking, supplemented with slashing insurance, which enhances the system's capital efficiency. The balance of stETH tokens is calculated based on the ether deposited into Lido, including total rewards and penalties. Due to the separation of the beacon chain and the Ethereum 1.0 network, Lido smart contracts cannot directly access beacon chain data. Instead, Lido DAO-appointed oracles monitor node operators' beacon chain accounts and relay the data to Lido's Ethereum 1.0 smart contracts.

Oracle Monitoring and stETH Recalculation

Whenever the oracle submits an update, the system recalculates the stETH token ratio. If staking rewards exceed slashing penalties, the system registers a profit, increasing the stETH token balances, and Lido applies a 10% fee. This fee is applied by minting stETH tokens equivalent to 10% of Lido's profit, which are then distributed between node operators and the DAO's treasury. The node operators' share of the fee is allocated proportionally to their active validation keys on the beacon chain. To mitigate the negative impact of slashing penalties on stETH token balances, part of the Lido fee is allocated to a slashing insurance provider. In the event of significant slashing incidents, Lido DAO governance is required to intervene.

Lido – protocol governance model

Governance process



Governance high level overview

Lido's governance model is centered around a dual governance framework designed to balance the interests of both LDO token holders and stETH holders. By allowing stETH holders to veto potentially harmful decisions, Lido ensures that any governance action is not only in the best interest of LDO token holders but also protective of staked assets.

LDO Governance:

LDO token holders are the primary decision-makers within the Lido protocol. They can propose and vote on a wide range of governance issues, including protocol upgrades, adjustments to the node operator registry, changes to staking rewards distribution, and modifications to the overall fee structure. Standard governance proposals require support from at least 5% of the total LDO supply to pass, while less critical changes can be expedited through an "Easy Track" motion, which has a lower threshold and cannot enact significant protocol modifications.

stETH Holder Veto Power:

To mitigate the risks associated with unilateral governance by LDO holders, Lido has introduced a veto mechanism for stETH holders. This mechanism allows stETH holders to collectively veto any governance decision that they believe could negatively impact their staked assets. By locking their stETH in a dedicated escrow contract, stETH holders can initiate a veto state, preventing the execution of a governance action. This veto can only be lifted if a subsequent anti-veto vote passes, where stETH holders vote to allow the action.

Lido – Key investors and funding rounds

Key Investors and Funding Rounds

Lido has raised a total of $167M in funding over 5 rounds, with initial coin offering on January 2021.Here are some of the investors:

- **Angel**: Zaki Manian, Viktor Bunin, Tim Beiko, Mariano Conti, Fernando Martinelli, Jinglan Wang, 0xMaki, Larry Sukernik, Derek Hsue, Elias Simos, Eric Wall, Ameen Soleimani, Ivan Golovko
- **Undisclosed Venture Rounds**: Andreessen Horowitz, Robot Ventures, Three Arrow Capital, Alameda Research, Jump Trading, Divergence Capital, Digital Currency Group, Delphi Ventures, Multicoin Capital, Dragonfly Capital, Coinbase Ventures, Paradigm,

dYdX

Business Case Study: dYdX

dYdX – general overview (1/2)

Company name: dYdX

- **Headquarters Regions :** San Francisco, United States
- **Founded Date :** July, 2017
- **Founders :** Antonio Juliano
- **Funding and Valuation:** Valuation of $0.66B (series C)

General Overview

dYdX is a decentralized exchange (DEX) specializing in derivatives trading, including perpetual contracts, margin trading, and spot trading. dYdX combines the transparency and security of decentralized finance with the advanced functionalities typically found in traditional financial markets. The platform's use of layer-2 scaling technology has made it one of the most efficient and user-friendly DEXs in the DeFi space.

History of dYdX: A Brief Overview

Founded in August 2017 by ex-Coinbase engineer Antonio Juliano, dYdX quickly established itself as a leading decentralized exchange (DEX) in the cryptocurrency space. The platform began by introducing advanced trading features such as margin trading and derivatives and soon marked its niche in the DeFi ecosystem. In its early stages, dYdX leveraged Ethereum smart contracts for its spot and margin trading products, allowing users to trade major cryptocurrencies like BTC and ETH with up to 5x leverage, while remaining fully non-custodial. However, the limitations of Ethereum's network, particularly high gas fees and slow transaction speeds during peak activity, led the team to seek a more scalable solution.

To address these challenges, dYdX shifted to Layer 2 via Starkware's zero-knowledge rollups in 2021 to enhance its transaction speed and reduce fees. This allowed the platform to offer higher leverage options, additional trading pairs, and cross-margin capabilities, with a heavy focus on perpetual contracts as the most popular product. In 2023, dYdX took a major step toward full decentralization with the launch of its own blockchain, dYdX Chain. With the recent rollout of v4, the platform now boasts a fully decentralized order book and matching engine, offering users faster transaction speeds and eliminating centralized trading fees.

dYdX – general overview (2/2)

Founder profile

Antonio Juliano

Antonio graduated from Princeton University with a degree in Computer Science. Before founding dYdX, Juliano worked at Coinbase as a software engineer and later as an engineer at Uber. His experience in both traditional finance and the crypto space has been instrumental in shaping dYdX.

Vision and mission

dYdX's vision is to become the leading DEX for perpetual contracts by building a fully decentralized, community owned trading platform. With the launch of its own sovereign chain, dYdX aims to provide users the trading experience that rivals centralized exchanges while providing transparency and and autonomy. With tokenomics that reward and engage users through staking and trading rewards, the platform creates a strong alignment between traders and the protocol's success.

Business model high level overview

1 Brief Description

DEX in perpetual futures and margin trading that leverages an order book model on its Layer-2 app chain.

2 Staking

Users can stake DYDX tokens to secure the network and earn trading rewards, creating a positive feedback loop.

3 Trading

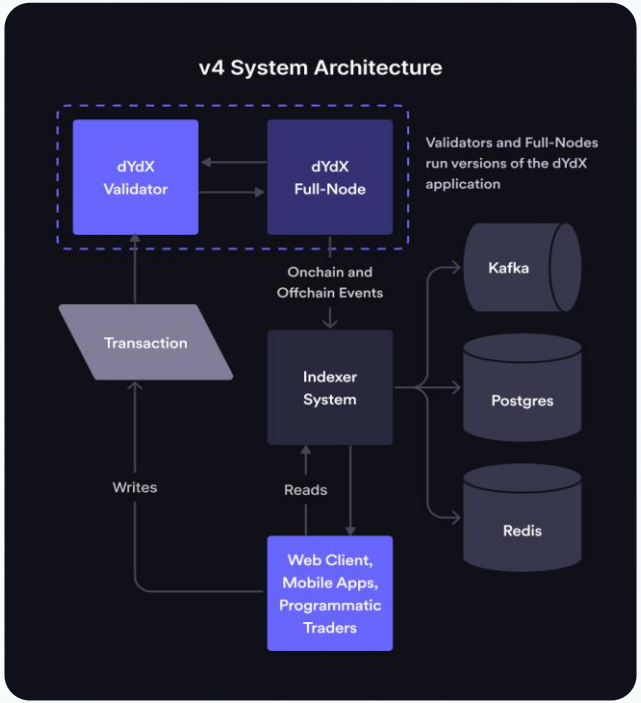
Access to perpetual futures contracts with up to 20x leverage, including cross-margin options and positions with no expiration.

4 Order Book Liquidity

An order book model is supported by deep liquidity and faster trade execution compared to AMM-based DEXs.

dYdX – business model high level characteristics

Business model characteristics



Order Lifecycle

At the core of dYdX's business model is the **decentralized validator and full-node network**. Validators and full nodes run the dYdX application, with validators being responsible for block production and order matching, while full nodes handle transaction gossiping and indexing. Validators are incentivized through trading fees, which are distributed based on the amount of dYdX tokens staked to their node. Full nodes support validators by processing blocks and serving data to indexers, creating a decentralized trading ecosystem.

Trading Process:

Transaction Submission – Users place their trades through various interfaces (e.g., web clients, mobile apps, APIs), which are then routed to a dYdX validator.

Order Matching – Validators manage off-chain order books to match buy and sell orders Once an order is matched, it is added to a proposed block. Validators then submit the block for consensus.

Consensus and Block Production – If at least two-thirds of the validators approve the block, it is committed to the blockchain.

Data Indexing – After the block is committed, data from the blockchain is indexed and made available to users through the Indexer system. This data includes on-chain and off-chain transaction details

User Interface – Users access the platform through decentralized front-ends. These interfaces interact with the Indexer to display trading data and execute new trades.

dYdX – key features and development roadmap (1/2)

dYdX V3

Layer 2 Scalability with StarkWare

dYdX v3 was a key milestone for the platform, introducing Layer 2 scalability through StarkWare's zkSTARKS technology. This zero-knowledge rollup solution significantly increased transaction throughput while reducing gas fees and trading costs. Built on Ethereum, dYdX v3 allowed users to trade perpetual contracts with greater efficiency, addressing the growing demand for high-speed, low-cost DeFi trading solutions.

Cross-Margined Perpetual Contracts

One of the central features of dYdX v3 is its cross-margined perpetual futures. These allow users to trade crypto derivatives without needing to hold the underlying asset, offering both long and short positions. The cross-margining system lets traders use profits from one position to cover potential losses from another, providing greater flexibility and the ability to maximize capital efficiency in volatile markets.

Non-Custodial Trading

Through StarkWare's ZK-Rollup technology, dYdX v3 offers fully non-custodial trading. This means users maintain full control over their assets, with trades settled off-chain but verified on-chain. The platform's integration of StarkEx for on-chain data availability and proof verification ensured that all trades were validated without the risk of custody vulnerabilities.

Reduced Gas Fees and Faster Transactions

By moving trade execution off-chain with zkSTARKS and Layer 2 scaling, dYdX v3 drastically reduced gas fees, which are often a barrier for active traders on Ethereum.

Mobile Trading

In addition to its web platform, dYdX v3 also launched mobile trading apps for iOS, providing users in eligible jurisdictions with the ability to trade perpetual contracts on the go.

dYdX – key features and development roadmap (2/2)

dYdX V4

Full Decentralization

With the launch of dYdX v4, the protocol is transitioning to a fully decentralized structure. This upgrade eliminates all central points of control, including dYdX Trading Inc.'s role in operating the order book and matching engine. Instead, dYdX v4 is built on its own Layer 1 blockchain powered by Cosmos SDK, with validators operating the off-chain order book and matching engine. The platform will now be entirely governed and managed by the community.

Off-Chain Order Book and Matching Engine

A key innovation of dYdX v4 is its off-chain order book and matching engine. Orders are gossiped between validators, and when they intersect, the matching engine processes the transaction, improving scalability. By handling orders off-chain, dYdX can support high-frequency trading with thousands of orders per second and without sacrificing decentralization.

Cosmos-Based Architecture

The shift to a Cosmos SDK-based blockchain enables dYdX to operate as a sovereign decentralized chain. Validators on dYdX Chain ensure the smooth functioning of the protocol using CometBFT Proof-of-Stake (PoS) consensus. This setup enables high transaction throughput while still offering decentralized governance. The transition to Cosmos also allows customization of gas fees, with users only paying fees when orders are matched.

Community-Driven Ecosystem

In dYdX v4, the community holds full control over the protocol's direction. As part of this decentralization, a "Community Tax" may be introduced on trading fees, with the option to direct these funds towards ecosystem growth or other initiatives. The community now plays a crucial role in driving innovation, managing updates, and ensuring the longevity of the protocol, making dYdX a truly decentralized trading platform with long-term sustainability.

dYdX – an overview of product technology

dYdX is a decentralized platform focused on providing advanced trading solutions for derivatives, leveraging the strengths of blockchain technology to enhance security, liquidity, and user experience. The platform aims to create a secure, efficient, and user-friendly environment for trading derivatives, such as perpetual contracts and margin trading, while incorporating cutting-edge technological innovations. Below is an elaboration on their mission and the technology they employ.

Perpetual Contracts:

- Functionality: Perpetual contracts on dYdX allow traders to maintain their positions for as long as they wish, without a predefined settlement date. The platform uses a funding rate mechanism, where periodic payments are made between long and short position holders to keep the contract price aligned with the underlying asset's spot price.
- Advantages: This model provides flexibility and continuous trading opportunities, attracting both short-term and long-term traders.

Smart Contracts:

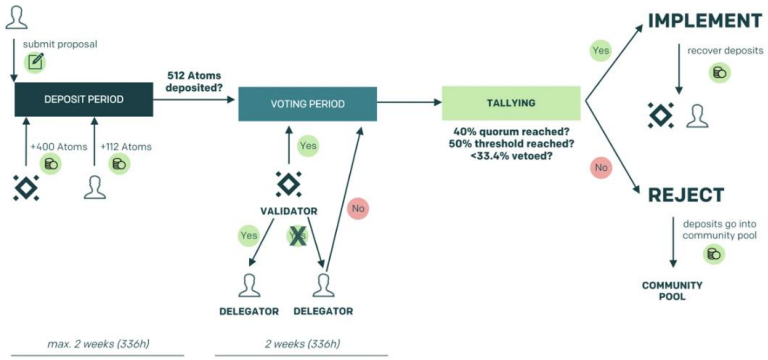
- Role: Smart contracts on dYdX are responsible for the execution of trades, settlement of positions, and management of collateral. These contracts ensure that the platform operates in a decentralized manner, minimizing the risk of centralized control or manipulation.
- Security: The use of audited and secure smart contracts helps to safeguard users' funds and maintain the integrity of the platform. All operations are transparent and verifiable on the blockchain.

Margin Trading:

- Functionality: Margin trading on dYdX allows users to borrow assets to increase their position size, amplifying potential profits with the use of leverage. Traders deposit collateral and can borrow funds to open larger positions, with the possibility of leveraging up to 20x on specific assets.
- Advantages: The integration of cross-margin trading allows users to manage multiple positions simultaneously, reducing the risk of liquidation by sharing collateral across trades.

dYdX – protocol governance model (1/2)

Governance process



dYdX Chain employs a governance model based on the Cosmos SDK's governance module. This decentralized governance system empowers token holders, validators, and stakers to submit proposals, vote on changes, and influence key decisions.

Unlike traditional governance models seen on Ethereum-based chains, this governance system relies heavily on validators. While some argue that governance should be more community-driven, dYdX allows for a balanced approach by enabling stakers to influence decisions while maintaining the chain's security and integrity through validators.

Step 1

Proposal Submission and Deposit

The governance process starts with any user submitting a proposal to the chain, and such a proposal must be backed by an initial deposit of DYDX tokens. This mechanism helps deter spam and low-quality submissions by requiring a certain level of commitment from the proposer. The minimum deposit is determined by the governance parameters, currently set at 10k DYDX tokens during the testnet phase.

Step 2

Voting Period and Participation

The proposal moves to the voting period, which lasts for seven days. During this time, validators and stakers participate in the voting process. Validators, who are responsible for securing the network, have the primary role of voting on proposals. Their votes are often inherited by the stakers who delegate their tokens to these validators. A key feature of the dYdX governance system is that stakers inherit the voting power of their validator, but they have the option to exercise their individual preferences by overriding the validator's vote. This hybrid approach balances efficiency (through validator voting) with individual autonomy (through manual overrides)

dYdX – protocol governance model (2/2)

Governance process Cont'd

Step 3

Quorum, Thresholds, and Implementation

Once the voting period ends, the protocol checks if a quorum has been reached, which requires at least 33.4% of staked tokens to have participated in the vote. If the quorum is not met, the proposal is automatically rejected. If quorum is met, the outcome is determined based on a 50%+ majority approval threshold. If the proposal secures more than half of the votes in favor and less than 33.4% of votes veto it, it is implemented.

The governance model ensures that only proposals with broad support from the community are passed. At the same time, governance parameters such as the quorum threshold, veto percentage, and deposit amounts can themselves be adjusted through governance proposals, providing a flexible, self-regulating system.

SubDaos

SubDAOs are smaller, specialized working groups within the broader DAO, each tasked with handling specific responsibilities that require domain-specific expertise. This ensures that decisions in areas such as risk management, technical infrastructure, and grants distribution are made efficiently and by knowledgeable community members, preventing the central DAO from being overwhelmed by a wide range of responsibilities.

There are two primary subDAOs:

The **Operations subDAO** is responsible for maintaining the technical infrastructure for dYdX v4 and supporting the ecosystem's growth. This includes managing key infrastructure like front-ends, indexers, and other technical components that ensure smooth operations.

The **Grants subDAO** focuses on the grants program, distributing funds to projects that contribute to the dYdX ecosystem. So far, it has overseen more than 120 grants, providing over $4M in funding to support various teams and initiatives that help expand and innovate the platform.

As dYdX Chain evolves, new subDAOs may be required to handle emerging responsibilities. For instance, subDAOs focused on risk management, incentives programs, and validator management could streamline operations in these areas.

dYdX – Key investors and funding rounds

Key Investors and Funding Rounds

dYdX has raised over $87M across multiple funding rounds. Its most recent Series C round it secured $65M.
Here are some of the investors:

- **Seed**: Andreessen Horowitz, Polychain, Christopher Golda, David King, Abstract Ventures, Avichal Garg, Caffeinated Capital, Brain Armstrong, 1confirmation, Scott Belsky, Platinum Capital, Jack Herrick, CSC Upshot, Kindred Ventures, Fred Ehrsam
- **Series A:** a16z Crypto, Polychain, Fred Ehrsam, Elad Gil, Raval Ravikant, Dragonfly, 1confirmation, Capitoria, Vy Capital, Abstract Ventures, Craft Ventures, Kindred Ventures, Bain Capital Ventures, Kevin Hartz
- **Series B**: DeFiance Capital, Three Arrows Capital, GSR, Wintermute Ventures, The Spartan Group, Polychain, RockTree Capital, Hashed, Scalar Capital, Andreessen Horowitz
- **Series C**: Paradigm, Hashkey Exchange, StarkWare Industries, Delphi Ventures, Andreessen Horowitz, Menai Financial Group, CMS Holdings, Kronos Research, QCP Capital, Toy Ventures, Finlink Capital, Abstract Ventures, CMT Digital Ventures, Three Arrows Capital, Wintermute Ventures, Electric Capital, Sixtant, mgnr.io, Polychain

06

Key challenges and opportunities towards the goal of mass adoption of decentralized finance technologies

Select benefits and challenges in the mass adoption of DeFi (1/2)

MARKET TRANSPARENCY AND AUDITABILITY

Utilizing open-source software and distributed ledgers enhances decentralization, programmability, and composability, thereby facilitating more efficient and cost-effective delivery of financial products and services compared to conventional finance. DeFi has the potential to decrease transaction costs, speed up transactions, and reduce errors, which can enhance financial efficiency and liquidity. Furthermore, the inherent transparency of DeFi's publicly accessible ledgers fosters trust among users and regulators, facilitating improved market transparency, auditability, and compliance enforcement.

DECENTRALIZATION

DeFi could bolster financial system resilience by diminishing dependence on "too-big-to-fail" entities through greater diversity and decentralization. By spreading financial services across a wider network of participants and technologies, DeFi can mitigate systemic risks and promote healthier market competition, ultimately reinforcing financial stability. Moreover, DeFi has the potential to dismantle barriers to financial access and inclusion by providing affordable, accessible financial services globally.

PRODUCT INNOVATION

The programmable nature of DeFi platforms fosters innovation and competition by enabling rapid experimentation and integration of novel financial products and services, potentially driving broader economic development and promoting digital inclusion. DeFi platforms are built on programmable blockchain networks like Ethereum, allowing developers to create new financial products and services through smart contracts. This programmability fosters innovation and enables the creation of financial instruments such as decentralized exchanges (DEXs), lending and borrowing protocols, trading and insurance with better terms and conditions.

ERRORS IN CODE AND PROGRAMMING

The reliance on open-source software, smart contracts, and decentralized protocols exposes DeFi to operational, technological, and security vulnerabilities, including coding flaws, cyberattacks, and liquidity discrepancies that can lead to substantial financial losses and market instability. Vulnerabilities in open-source software, coupled with the automated execution of smart contracts, can trigger systemic failures during periods of market stress or coding errors, reminiscent of historical financial crises.

Select benefits and challenges in the mass adoption of DeFi (2/2)

DECENTRALIZED GOVERNANCE STRUCTURES

Decentralized governance structures harbor conflicts of interest that obscure accountability, compounding risks for less sophisticated participants. Furthermore, market integrity is compromised by prevalent conflicts of interest and the pseudo-anonymous nature of transactions within DeFi ecosystems. These factors facilitate practices like wash trading, front running, and pump-and-dump schemes, undermining market fairness and eroding investor confidence. Insufficient governance mechanisms and regulatory oversight exacerbate these risks, hampering effective responses to illicit activities.

ANONYMITY IN TRANSACTIONS

The anonymity and cross-border nature of DeFi transactions pose challenges in combating illicit finance activities like money laundering and terrorist financing. The decentralized and permissionless nature of these networks complicates traditional regulatory frameworks and international efforts to enforce sanctions and maintain financial oversight capabilities.

07

Decentralized finance technology key legal, jurisdictional and regulatory considerations

DeFi technology select legal, jurisdictional and regulatory issues (1/3)

DISTRIBUTED LEDGER TECHNOLOGY (DLT)

Advances in cryptography and computing power have had a profound impact on digital ledgers, leading to the rise of Distributed Ledger Technology (DLT). DLT allows for the creation of shared and unchangeable records of ownership without the need for a central authority, relying on cryptographic algorithms for achieving consensus among participants. This technological breakthrough has paved the way for the emergence of crypto assets and decentralized finance (DeFi), revolutionizing the financial landscape by enabling novel services like peer-to-peer borrowing and lending without the involvement of traditional intermediaries. Moreover, DLTs are being increasingly considered for their potential to streamline the representation and transfer of traditional assets in a more efficient manner. Despite offering numerous benefits, these advancements also come with inherent risks such as heightened market volatility, operational hurdles, and uncertainties surrounding regulation. Policymakers face the daunting task of devising robust regulatory frameworks that strike a delicate balance between fostering innovation, safeguarding consumer interests, and preserving financial stability in the face of rapid technological evolution.

JURISDICTION

A lot of intricate challenges are associated with defining and categorizing crypto assets and their related activities in different jurisdictions. The absence of universally accepted definitions for terms like "crypto asset," leads up to a mix-up in the usage of terms such as digital assets, cryptoassets, virtual assets, and crypto tokens. Regulatory bodies and authorities employ diverse taxonomies based on technical, functional, and legal considerations. There are three dimensions that can be utilized for the classification of policy measures: crypto asset activities, how these activities are managed, and the specific types of crypto assets involved. Crypto asset activities are divided into issuance, operations involving Distributed Ledger Technology (DLT) infrastructure, and services connected to crypto assets. Additional supporting activities like code development and risk advisory services are also taken into account. In terms of management, a distinction can be made between activities that are centrally managed and those that are overseen by a community within public DLT networks. The numerous types of crypto assets include digital assets primarily issued by private entities, predicated on cryptographic techniques and distributed ledger technology. These assets serve various purposes, ranging from access to services, developing applications on DLT platforms, or representing ownership stakes in physical assets like gold. In short, a lot of complexities are inherent in comparing regulatory responses across different countries due to the absence of standardized terminology and classification systems.

DeFi technology select legal, jurisdictional and regulatory issues (2/3)

At the jurisdictional level, authorities exhibit varying responses to stablecoins used for investments, with most not yet implementing specific initiatives due to uncertainties about the associated risks and appropriate regulatory frameworks. Some jurisdictions, like Switzerland's FINMA, have categorized stablecoins based on their underlying assets, subjecting them to pertinent financial laws. The European Union has introduced a specialized regime for stablecoins used primarily as investments, known as Asset-Referenced Tokens (ART). This framework imposes stringent requirements on issuers, including licensing, capital reserves, risk management, and provisions for orderly wind-downs. It also mandates strict rules for white paper disclosures. Internationally, the International Organization of Securities Commissions (IOSCO) has analyzed stablecoins as potential regulated securities or financial instruments, aligning them with existing standards for money market funds or exchange-traded funds, depending on their structure. Overall, while some jurisdictions are developing specific regulations, others remain cautious, emphasizing the need for thorough risk assessments and regulatory adaptation. The international landscape reflects ongoing efforts to ensure consistent and comprehensive oversight of stablecoin activities to safeguard financial stability.

TOKENS AND DECENTRALIZED FINANCE PROTOCOLS

Native tokens are created on public distributed ledger technologies (DLTs) like blockchains through consensus mechanisms, serving various functions such as peer-to-peer payments (e.g., Bitcoin) or as utility tokens within specific platforms (e.g., Ethereum). Regulatory approaches to native tokens vary, with some jurisdictions classifying them as virtual assets subject to financial services regulations, while others assess them under securities laws, such as the Howey Test in the United States. DeFi protocols, on the other hand, operate on public DLTs using smart contracts to provide financial services such as lending and exchanging without traditional intermediaries. These protocols are governed by decentralized communities, although some aspects like governance and ownership may still exhibit centralization. DeFi presents regulatory challenges due to risks associated with money laundering, terrorism financing, and investor protection, stemming from its anonymous nature and lack of traditional safeguards. Regulatory responses to these challenges include providing clarifications on applicable laws, enforcement actions, and cautious integration of DeFi into regulated financial systems. Policymakers worldwide are issuing guidelines, clarifications, and enforcement measures tailored to address the risks associated with native tokens and DeFi protocols. Examples include licensing requirements for decentralized exchanges and staking activities in Dubai. International coordination efforts, such as the Financial Action Task Force's (FATF) guidelines on virtual assets and DeFi, underscore the need for a unified global approach to mitigate risks related to anti-money laundering (AML) and counter-terrorism financing (CFT). It is important to understand these technologies, clarify regulatory frameworks, and implement measures to protect users and ensure financial stability.

DeFi technology select legal, jurisdictional and regulatory issues (3/3)

USERS AND POLICY MEASURES

Policy measures today are aimed at mitigating the risks associated with users' direct exposures to crypto assets and related activities. Users can be categorized into retail investors (such as households and non-financial firms) and wholesale investors (including financial institutions and institutional investors). For retail investors, authorities frequently issue warnings to protect them from the risks associated with specific types of crypto assets, such as Bitcoin and Ethereum. These warnings aim to educate consumers about the potential dangers involved. Additionally, various jurisdictions have banned certain crypto asset derivatives and imposed restrictions on promotional activities to further safeguard retail investors. As the popularity of both native and non-native tokens has surged, there has been a corresponding increase in warnings about fraudulent schemes. Authorities are actively identifying and warning against fraudulent trading platforms. In terms of promotional practices, countries like Spain and the UK have introduced regulatory frameworks to govern the advertising of crypto assets, ensuring better consumer protection. For wholesale investors, policy initiatives focus on consumer protection risks and compliance standards for custody services. Regulations for institutional investors, including banks and investment funds, are designed to address these concerns. On an international level, the Basel Committee on Banking Supervision (BCBS) has developed risk-based classifications for crypto assets to guide the capital treatment by banks, with the implementation of these guidelines scheduled for 2025.

DeFi technology regulatory framework guideline

United States

Regulatory Framework Guideline

1. **Securities and Exchange Commission (SEC):** Focuses on whether DeFi projects involve securities offerings. Projects may need to register or qualify for an exemption.

2. **Commodity Futures Trading Commission (CFTC):** Oversees derivatives and commodities markets, potentially impacting DeFi platforms offering these products.

3. **Financial Crimes Enforcement Network (FinCEN):** Ensures compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations.

Key Developments

1. **SEC Enforcement Actions:** Increased scrutiny on DeFi projects that potentially offer unregistered securities.

2. **Proposed Legislation:** Efforts like the Digital Commodity Exchange Act aim to create a comprehensive framework for digital assets.

United Kingdom

Regulatory Framework Guideline

1. **Financial Conduct Authority (FCA):** Regulates financial markets and has issued guidance on crypto assets, focusing on AML and consumer protection.

2. **Bank of England (BoE):** Exploring the impact of DeFi on financial stability

Key Developments

1. **Crypto-asset Taskforce:** Collaboration between HM Treasury, FCA, and BoE to assess and regulate the crypto market.

2. **Consultations on Stablecoins:** Exploring regulatory frameworks for stablecoins, which are crucial for DeFi.

European Union

Regulatory Framework Guideline

1. **Markets in Crypto-Assets (MiCA) Regulation:** Regulation that aims to provide legal clarity and consumer protections while fostering innovation.

2. **European Securities and Markets Authority (ESMA):** Monitors financial stability and investor protection within the EU, potentially influencing DeFi regulation.

Key Developments

1. **MiCA Progress:** Consultation packages being launched in phases over few years with negotiations and adjustments to the MiCA proposal

DeFi technology regulatory framework guideline

China

Regulatory Framework Guideline

1.People's Bank of China (PBoC): Leads the regulation of digital currencies and has banned most crypto activities, including trading and ICOs.

2.Cyberspace Administration of China (CAC): Oversees blockchain-related projects, ensuring compliance with stringent regulations.

Key Developments

1.Digital Yuan: Development and trial of the Digital Currency Electronic Payment (DCEP) system, which contrasts with decentralized currencies.

2.Crackdown on Crypto Mining and Trading: Continued enforcement actions against crypto activities, affecting DeFi indirectly.

Singapore

Regulatory Framework Guideline

1.Monetary Authority of Singapore (MAS): Progressive stance on digital assets, requiring licensing for crypto service providers under the Payment Services Act.

2.AML/CFT Requirements: Strict regulations to prevent money laundering and terrorist financing.

Key Developments

1.Project Ubin: Collaboration with financial institutions to explore blockchain technology for clearing and settlement.

2.Licensing Regime: Introduction of clear guidelines and licensing requirements for DeFi and crypto projects.

Japan

Regulatory Framework Guideline

1.Financial Services Agency (FSA): Regulates crypto exchanges and enforces AML/CFT measures.

2.Payment Services Act: Provides a framework for digital asset transactions.

Key Developments

1.JVCEA and JVCEA II: Self-regulatory organizations working closely with the FSA to oversee the crypto industry.

2.Stablecoin Regulation: Discussions on creating a framework for stablecoin issuance and use in DeFi.

08

Decentralized finance technologies select industry use cases and key benefits

Decentralized finance technologies select business case studies (1/6)

Stablecoins

Definition	Stablecoins serve as a bridge between the volatile cryptocurrency world and the stable value of fiat currencies, primarily aiming to mirror the U.S. dollar. They offer a stable medium of exchange and a reliable store of value, mitigating the high volatility associated with digital assets.
Particulars	○ *Custodial Stablecoins:* These are backed by fiat currencies or other assets held in reserve by a central custodian, like USDC or the proposed Diem by Facebook. ○ *Asset-backed Stablecoins:* These stablecoins use a variety of assets as collateral that are managed through smart contracts. The collateral can be other cryptocurrencies or tokenized real-world assets, and the stablecoin's value is maintained by dynamic collateral management. ○ *Algorithmic Stablecoins:* These operate through algorithms that automatically adjust the supply of the stablecoin based on its price fluctuations relative to its peg. This method does not require physical reserves.
Case Study	*Example: MakerDAO and DAI Stablecoin* DAI is a decentralized stablecoin that is part of the MakerDAO ecosystem that operates on the Ethereum blockchain. It maintains a stable value against the U.S. dollar by allowing users to deposit various cryptocurrencies as collateral in a Maker Vault. Users receive DAI in return and take out a loan that must be over-collateralized to guard against market fluctuations. The stability of DAI is managed through an automated system that liquidates the vault if the collateral's value falls below a certain threshold.

Decentralized finance technologies select business case studies (2/6)

Exchanges

Definition	Exchanges enable the trading of digital assets, which are crucial for both the utilization of DeFi services and the potential profit from the appreciation of such assets. Unlike centralized exchanges that require trust in an intermediary to manage the trades, custody funds, and ensure fair pricing, DeFi exchanges operate on a trust-minimized basis with the help of blockchain technology.
Particulars	○ *Decentralized Order Books:* These exchanges operate similarly to traditional exchanges but on a decentralized platform with order books maintained on-chain. This setup enhances security but can face challenges like higher gas fees and slower transactions ○ *Automated Market Makers (AMMs):* AMMs discard the traditional order book entirely. Instead, they use algorithms to price assets based on the available liquidity in their pools. This mechanism allows for continuous liquidity and trading without the need for matching buyers with sellers. Liquidity providers supply the pools with funds and earn yield from trading fees.
Case Study	*Example: Uniswap and Sushiswap* Uniswap is a pioneering AMM protocol built on Ethereum. It employs a simple formula xy=k to ensure that the product of the quantities of two swapping tokens remains constant, thus determining the price automatically. When a trade is made, it shifts the ratio of tokens in the pool and affects the price. SushiSwap originated as a fork of Uniswap and introduced a governance token called SUSHI to allow holders to vote on protocol changes. It differentiates itself by allocating a portion of the trading fees to SUSHI token holders to enhance the potential for earnings through governance participation

Decentralized finance technologies select business case studies (3/6)

Credit

Definition	Credit is transformed through decentralized credit protocols in DeFi, unlike in traditional finance where banks act as the intermediaries, managing credit risks and the spread between the interest clients pay and receive. Interest rates are based on the supply-to-borrowing ratio as lenders provide capital to a pool and receive tokens that accrue interest over time. This system is different from traditional banking as it allows both lenders and borrowers to retain custody of their assets, with terms that can be adjusted dynamically by the protocol's governance mechanisms.
Particulars	○ *Collateralization:* DeFi loans are typically overcollateralized, requiring borrowers to lock up collateral worth more than the loan amount. This guards against the high volatility. Interest Rates: Interest rates in DeFi credit markets are dynamic, adjusting algorithmically based on the current supply and demand for different assets. ○ *Flash Loans:* A unique feature that allows users to borrow substantial sums without collateral, provided they repay within the same transaction block. Typically used for arbitrage, collateral swaps, and market manipulation, these loans demonstrate both the innovative and risky aspects of DeFi.
Case Study	*Example: Compound* Compound is a DeFi credit protocol where users can lend or borrow assets instantly through a smart contract system. The platform issues a COMP governance token that enables holders to vote on critical protocol decisions such as interest rate models and the types of supported collateral. Compound also popularized "liquidity mining," distributing COMP tokens to active lenders and borrowers to incentivize participation and investment in the platform.

Decentralized finance technologies select business case studies (4/6)

Derivatives

Definition	Derivatives in traditional finance involve multiple intermediaries like futures commission merchants and central clearinghouses to manage orders, secure transactions, and mitigate counterparty risks. In DeFi, derivatives are executed through protocols that eliminate the need for central intermediaries. Instead, they use smart contracts to connect buyers and sellers directly, where trades are backed by collateral pools and governed by protocol participants. These platforms can also support leverage to magnify returns or provide tools for betting against asset prices, and even host prediction markets that aggregate collective forecasts on future events.
Case Study	*Example: Synthetix* Synthetix is a synthetic asset issuance protocol on the Ethereum blockchain, enabling users to trade synthetic versions of various assets. Users stake the native SNX token to create 'Synths', which mimic the price movements of real-world assets, allowing for overcollateralized derivatives trading. This system opens up access to global assets which might be restricted in certain regions, offering broad exposure while collecting trading fees for token holders

Decentralized finance technologies select business case studies (5/6)

Insurance

Definition	Insurance in DeFi introduces decentralized insurance pools that leverage blockchain technology to manage and mitigate unique digital risks such as smart contract failures and protocol hacks. It operates through pools of digital assets, where capital providers collateralize the pool in return for tokens that represent a share of the premiums. This model eliminates the need for traditional insurance intermediaries by using smart contracts for policy management and claims processing. Claims are assessed and voted on by token holders, ensuring a decentralized governance structure.
Case Study	*Example: Nexus Mutual* NexusMutual is a platform offering smart contract insurance, charging an annual fee for coverage against risks like smart contract bugs, with payouts in ETH or DAI based on community votes. It also covers risks associated with centralized financial platforms.

Decentralized finance technologies select business case studies (6/6)

Asset Management

Definition	Asset management leverages smart contracts to manage diversified portfolios of digital assets, including tokens that represent traditional assets, synthetic assets, and interest-bearing accounts. These assets operate similarly to traditional asset management structures but without the need for intermediaries like custodians or brokers. This shift blurs the lines between different asset classes and traditional financial service models.
Case Study	*Example: Set Protocol* Set Protocol is a decentralized platform that allows users to create tokenized portfolios, which are collections of various digital assets including cryptocurrencies like Bitcoin and Ethereum, as well as stablecoins. Sets can automatically rebalance based on predefined conditions such as time intervals or price deviations.

References and report citations

The investment white paper report has been prepared using internal analysis as well as information sourced from various sources. Here are some of the links for the report references and citations that were used as part of the preparation of the research report:

i. https://keyrock.com/future-real-world-asset-tokenization/
ii. https://www.ledger.com/academy/topics/defi/what-is-aave
iii. https://cryptowallet.com/academy/aave-use-case/
iv. https://www.lemma.solutions/insights/aave-governance-v3-case-study
v. https://medium.com/`coinmonks/unleashing-the-power-of-defi-building-a-lending-and-borrowing-platform-like-aave-fe81c5304e88
vi. https://rdi.berkeley.edu/berkeley-defi/assets/material/Dan%20Robinson%20Lecture%20Slides.pdf
vii. https://boilerblockchain.medium.com/industry-case-study-uniswap-b0293ec44ef2
viii. https://docs.uniswap.org/concepts/research
ix. https://members.delphidigital.io/projects/lido
x. https://cointelegraph.com/learn/what-is-lido-liquidity-for-staked-assets
xi. https://www.bitstamp.net/learn/cryptocurrency-guide/what-is-lido-ldo/
xii. https://www.coindesk.com/learn/what-is-dydx-understanding-the-decentralized-crypto-exchange/
xiii. https://www.bitstamp.net/learn/cryptocurrency-guide/what-is-dydx/
xiv. https://cryptowallet.com/academy/dydx-use-case/

i. https://medium.com/@allenzhuer/how-to-analyze-defi-projects-d8d0a55a05de
ii. https://medium.com/@teamearlybird/analyzing-the-current-state-of-decentralized-finance-defi-319da7b5c306#:~:text=The%20Decentralized%20Finance%20(DeFi)%20industry,need%20for%20traditional%2C%20centralized%20intermediaries.
iii. https://www.bis.org/fsi/publ/insights49.pdf
iv. https://wifpr.wharton.upenn.edu/wp-content/uploads/2021/05/DeFi-Beyond-the-Hype.pdf
v. https://www.coinbase.com/learn/crypto-basics/what-is-defi#:~:text=DeFi%20takes%20the%20basic%20premise,trading%20floors%2C%20banker%20salaries).
vi. https://www.crypto-news-flash.com/top-defi-trends-in-2024/
vii. https://www.vpnranks.com/resources/blockchain-technology-statistics/
viii. https://b2bdaily.com/fintech/what-key-trends-will-shape-the-future-of-defi-in-2024/

GLOBAL MILLENNIAL CAPITAL

Global Millennial Capital Investment Research Team:

Andreea Danila
General Partner

Henry Sun
Investment Analyst

Tanushree Upreti
Venture Partner