**What Are Automated Market Makers (AMMs)?**

DEFINITION

Automated market makers (AMMs) are decentralized exchanges that use algorithmic “money robots” to provide liquidity for traders buying and selling crypto assets.

What is an automated market maker? Automated market makers (AMMs) are a type of [decentralized exchange (DEX)](https://chain.link/education-hub/what-is-decentralized-exchange-dex) that use algorithmic “money robots” to make it easy for individual traders to buy and sell crypto assets. Instead of trading directly with other people as with a traditional order book, users trade directly through the AMM.

Market makers are entities tasked with providing liquidity for a tradable asset on an exchange that may otherwise be illiquid. Market makers do this by buying and selling assets from their own accounts with the goal of making a profit, often from the spread—the gap between the highest buy offer and lowest sell offer. Their trading activity creates liquidity, lowering the price impact of larger trades.

While other types of decentralized exchange (DEX) designs exist, AMM-based DEXs have become extremely popular, providing deep liquidity for a wide range of digital tokens.

**What Are Liquidity Pools and Liquidity Providers?**

Underpinning AMMs are liquidity pools, a crowdsourced collection of crypto assets that the AMM uses to trade with people buying or selling one of these assets. The users that deposit their assets to the pools are known as liquidity providers (LPs).

Liquidity is essential for AMMs to function properly. If an AMM doesn’t have a sufficient liquidity pool, it can create a large price impact when traders buy and sell assets on the DeFi AMM, leading to capital inefficiency and impermanent loss. To incentivize liquidity providers to deposit their crypto assets to the protocol, AMMs reward them with a fraction of the fees generated on the AMM, usually distributed as LP tokens. The practice of depositing assets to earn rewards is known as [yield farming](https://chain.link/education/defi/yield-farming).

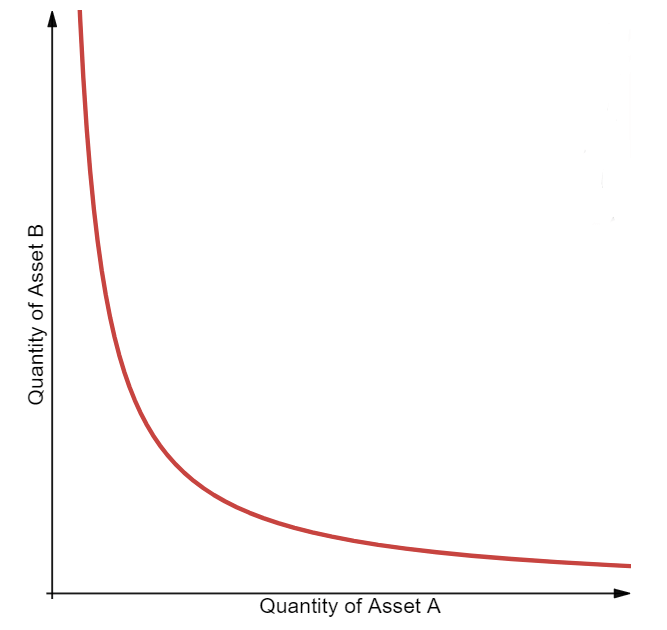
The prices of assets on an AMM automatically change depending on the demand. For example, a liquidity pool could hold ten million dollars of ETH and ten million dollars of USDC. A trader could then swap 500k dollars worth of their own USDC for ETH, which would raise the price of ETH on the AMM.

**What Are the Different Automated Market Maker (AMM) Models?**

Constant function market makers (CFMMs), such as constant product market makers, constant sum market makers, and constant mean market makers, are a class of first-generation AMMs made popular by protocols like Bancor, Curve, and Uniswap. These AMM exchanges are based on a constant function, where the combined asset reserves of trading pairs must remain unchanged. In non-custodial AMMs, user deposits for trading pairs are pooled within a [smart contract](https://chain.link/education/smart-contracts) that any trader can use for token swap liquidity. Users trade against the smart contract (pooled assets) as opposed to directly with a counterparty as in order book exchanges.

**Constant Product Market Maker (CPMM)**

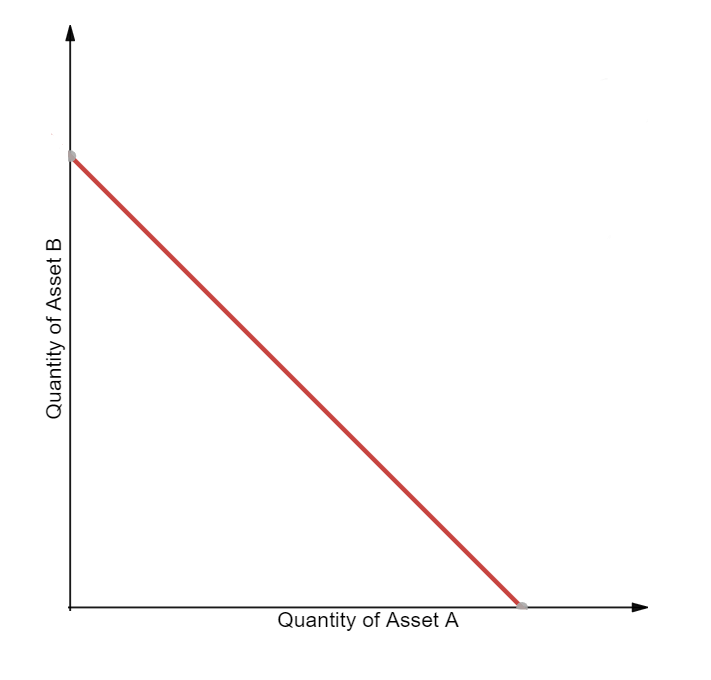
The first type of CFMM to emerge was the constant product market maker (CPMM), which was popularized by the first AMM-based DEX, Bancor. CPMMs are based on the function x\*y=k, which establishes a range of prices for two tokens according to the available quantities (liquidity) of each token. When the supply of token X increases, the token supply of Y must decrease, and vice-versa, to maintain the constant product K. When plotted, the result is a hyperbola where liquidity is always available but at increasingly higher prices, which approach infinity at both ends.



A visualization of a constant product market maker; source: Dmitriy Berenzon

**Constant Sum Market Maker (CSMM)**

The second type is a constant sum market maker (CSMM), which is ideal for zero-price-impact trades but does not provide infinite liquidity. CSMMs follow the formula x+y=k, which creates a straight line when plotted. This design unfortunately allows arbitrageurs to drain one of the reserves if the off-chain reference price between the tokens is not 1:1. Such a situation would destroy one side of the liquidity pool, leaving all of the liquidity residing in just one of the assets and therefore leaving no more liquidity for traders. Because of this, CSMM is a model rarely used by AMMs.



A visualization of a constant sum market maker; source: Dmitriy Berenzon

**Constant Mean Market Maker (CMMM)**

The third type is a constant mean market maker (CMMM), which enables the creation of AMMs that can have more than two tokens and be weighted outside of the standard 50/50 distribution. In this model, the weighted geometric mean of each reserve remains constant. For a liquidity pool with three assets, the equation would be the following: (x\*y\*z)^(⅓)=k. This allows for variable exposure to different assets in the pool and enables swaps between any of the pool’s assets.

**Problems of First-Generation AMM Models**

Many of first-generation AMMs are limited by impermanent loss and low capital efficiency, which impacts both liquidity providers and traders.

**Impermanent Loss**

Impermanent loss is the difference in value over time between depositing tokens in an AMM versus simply holding those tokens in a wallet. This loss occurs when the market-wide price of tokens inside an AMM diverges in any direction. Since AMMs don’t automatically adjust their exchange rates, they require an arbitrageur to buy the underpriced assets or sell the overpriced assets until the prices offered by the AMM match the market-wide price of external markets. The profit extracted by arbitrageurs is siphoned from the pockets of liquidity providers, creating a loss.

**Low Capital Efficiency**

Traditional AMM designs require large amounts of liquidity to achieve the same level of price impact as an order book-based exchange. This is due to the fact that a substantial portion of AMM liquidity is available only when the pricing curve begins to turn exponential. As such, most liquidity will never be used by rational traders due to the extreme price impact experienced.

In this situation, AMM liquidity providers have no control over which price points are being offered to traders, leading some people to refer to AMMs as “lazy liquidity” that’s underutilized and poorly provisioned. Meanwhile, market makers on order book exchanges can control exactly the price points at which they want to buy and sell tokens. This leads to very high capital efficiency, but with the trade-off of requiring active participation and oversight of liquidity provisioning.

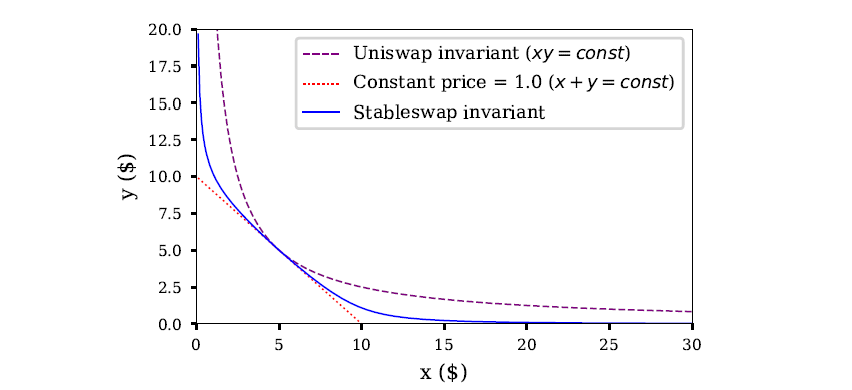
**Improving AMM Models With Hybrid, Dynamic, Proactive, and Virtual Solutions**

The above limitations are being overcome by innovative projects with new design patterns, such as hybrid automated market makers, dynamic automated market makers, proactive market makers, and virtual automated market makers.

**Hybrid CFMMs**

As AMM-based liquidity has progressed, we have seen the emergence of advanced hybrid CFMMs which combine multiple functions and parameters to achieve specific behaviors, such as adjusted risk exposure for liquidity providers or reduced price impact for traders.

For example, [Curve](http://curve.fi/) AMMs—known as the stableswap invariant—combine both a CPMM and CSMM using an advanced formula to create denser pockets of liquidity that bring down price impact within a given range of trades. The result is a hyperbola (blue line) that returns a linear exchange rate for large parts of the price curve and exponential prices when exchange rates near the outer bounds.



Source: Curve whitepaper‌‌

Hybrid CFMMs enable extremely low price impact trades by using an exchange rate curve that is mostly linear and becomes parabolic only once the liquidity pool is pushed to its limits. Liquidity providers earn more in fees (albeit on a lower fee-per-trade basis) because capital is used more efficiently, while arbitrageurs still profit from rebalancing the pool.

Curve offers low-price-impact swaps between tokens that have a relatively stable 1:1 exchange rate. This means its solution is predominantly designed for stablecoins. However, Curve has also recently launched support for more volatile token pairs with similarly concentrated liquidity.

**Dynamic Automated Market Maker (DAMM)**

Using a dynamic automated market maker (DAMM) model, [Sigmadex](https://sigmadex.org/" \t "_blank) leverages [Chainlink Price Feeds](https://chain.link/data-feeds) and implied volatility to help dynamically distribute liquidity along the price curve. By incorporating multiple dynamic variables into its algorithm, it can create a more robust market maker that adapts to changing market conditions. During periods of low volatility, Sigmadex can concentrate liquidity near the market price and increase capital efficiency, and then expand it during periods of high volatility to help protect traders from impairment loss.

**Proactive Market Maker (PMM)**

Also aiming to increase liquidity on its protocol, [DODO](https://dodoex.io/) is using a model known as a proactive market maker (PMM) that mimics the human market-making behaviors of a traditional central limit order book. The protocol uses globally accurate market prices from Chainlink Price Feeds to proactively move the price curve of each asset in response to market changes, increasing the liquidity near the current market price. Ultimately, this facilitates more efficient trading and reduces the impairment loss for liquidity providers.

**Virtual Automated Market Makers (vAMM)**

Virtual automated market makers (vAMMs) such as [Perpetual Protocol](https://perp.com/) minimize price impact, mitigate impermanent loss, and enable single token exposure for synthetic assets. vAMMs use the same x\*y=k constant product formula as CPMMs, but instead of relying on a liquidity pool, traders deposit collateral to a smart contract. By trading synthetic assets rather than the underlying asset, users can gain exposure to the price movements of a wide variety of crypto assets in a highly efficient manner. However, users holding an open position in a synthetic asset are at risk of having their collateral liquidated if the price moves against them.

**Chainlink Oracles Are Powering AMM Innovation**

[Chainlink Price Feeds](https://chain.link/solutions/defi) already underpin much of the DeFi economy and play a key role in helping AMMs accurately set asset prices and increase the liquidity available to traders. Now, [Chainlink Automation](https://chain.link/automation) is beginning to play a major role by enabling smart contracts to be automated in a decentralized and highly secure manner. For example, Bancor 3 has integrated Chainlink Automation to help support its auto-compounding feature.

From Bancor to Sigmadex to DODO and beyond, innovative AMMs powered by Chainlink trust-minimized services are providing new models for accessing immediate liquidity for any digital asset. Not only do AMMs powered by Chainlink help create price action in previously illiquid markets, but they do so in a highly secure, globally accessible, and non-custodial manner.

# What Are Flash Loans?

DEFINITION

A flash loan is a type of loan where a user borrows assets with no upfront collateral and returns the borrowed assets within the same blockchain transaction.

A flash loan is a type of uncollateralized loan that lets a user borrow assets with no upfront collateral as long as the borrowed assets are paid back within the same blockchain transaction.

The [decentralized finance (DeFi)](https://chain.link/education/defi) ecosystem started out by recreating traditional financial services, such as lending and borrowing, exchanges, futures and options markets, for blockchains. As the ecosystem developed, fundamentally new services were created that are only possible thanks to the inherent properties of blockchain technology and the [permissionless composability](https://chain.link/education-hub/permissionless-composability) enabled by smart contract applications.

Like the concept of [yield farming](https://chain.link/education/defi/yield-farming), flash loans are an exciting new financial primitive. Flash loans enable users to borrow assets from an on-chain liquidity pool with no upfront collateral as long as the borrowed amount of liquidity, plus a small fee, is returned to the pool within the same transaction. If the borrower does not pay back the loan in the same transaction, then the entire transaction is reverted, including the initial borrow and any actions taken afterward. This innovative mechanism increases access to capital for users across a variety of use cases while ensuring the continued solvency of the underlying on-chain liquidity pool.

In this article, we outline how flash loans work, what they are used for, and what DeFi protocols can do to mitigate the potential attack vectors created by this new financial primitive.

## How Do Flash Loans Work?

In the case of collateralized lending, borrowers need to put up capital (collateral) to borrow funds. If the borrower fails to meet the terms of the loan, the lender can still cover the loan using the borrower’s collateral. Flash loans don’t have this requirement; the loan can only exist if the borrower pays it back within the same transaction. As a result, defaulting on a flash loan is not possible, since the entire transaction would simply revert.

For a short period of time—the span of a single transaction—a flash loan can turn anyone into a very well-capitalized actor. The hundreds of millions of dollars of liquidity provided by flash loans creates unique opportunities for arbitrage, liquidations, collateral swapping, and the creation of leveraged positions. It also creates certain risks, especially for a nascent ecosystem of financial protocols with varying degrees of decentralization and security. These risks should be understood by smart contract developers so more robust applications can be built for users.

## What Are Flash Loans Used For?

The most common usage of flash loans is for arbitrage. By harnessing a large amount of capital to fill an inefficiency in the market, where an asset has differing exchange rates on different markets, arbitrageurs can generate a profit by bringing the market to an equilibrium and improving liquidity for everyone in the DeFi market.

Another use case for flash loans is liquidations. Many lending protocols incentivize third-party liquidators that can earn a reward for liquidating loans that fail to meet a certain collateralization ratio requirement. Access to large amounts of capital through flash loans can help ensure that undercollateralized loans are liquidated on time and the underlying protocol remains solvent.

Flash loans can also be used for collateral swaps—a technique where a user closes their loan with borrowed funds to immediately open a new loan with a different asset as collateral. Flash loans can also simplify the process of creating a leveraged position or allow loans to be seamlessly transferred across protocols.

## Flash Loans and Price Oracle Attacks

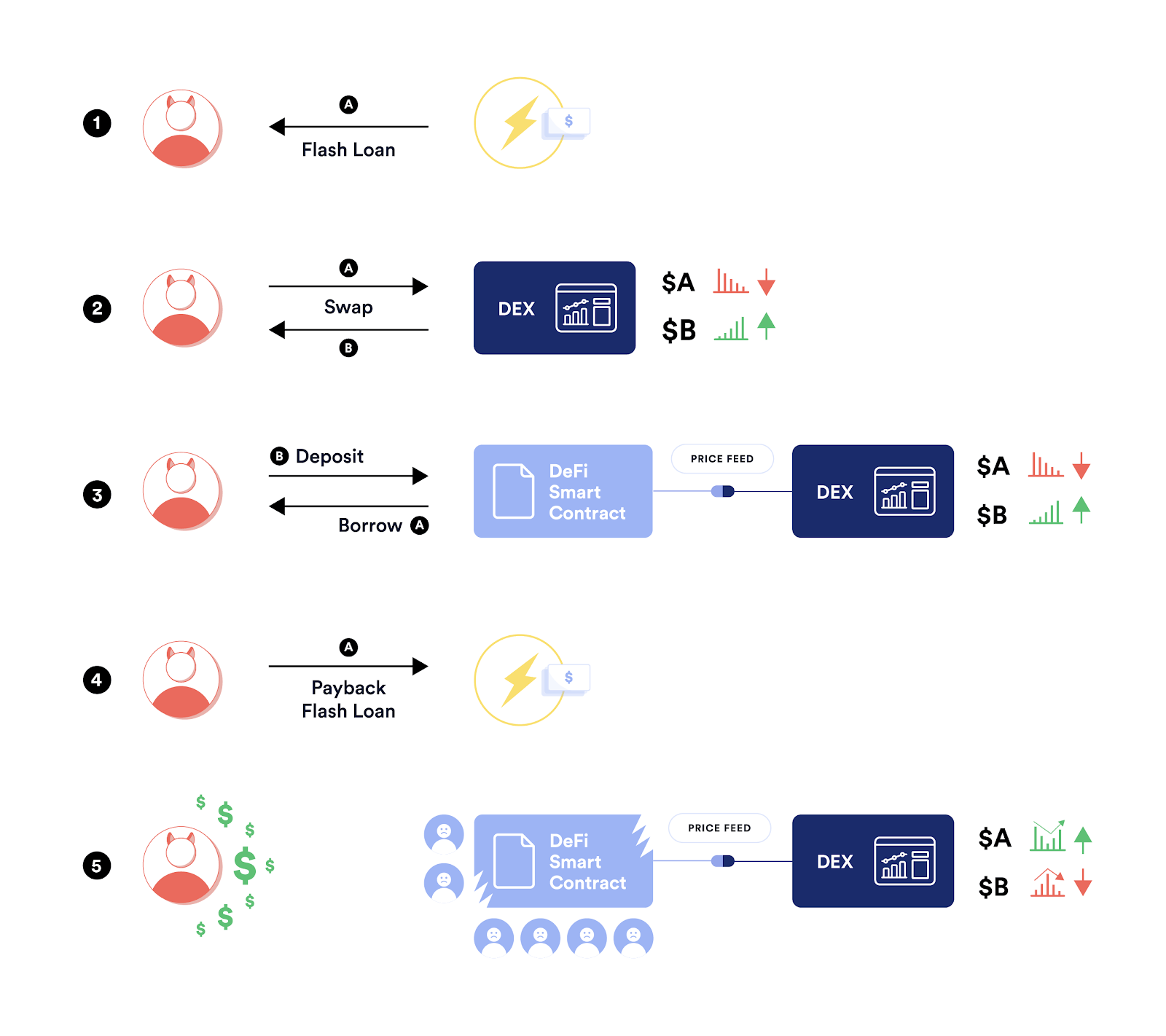
Flash loans have a controversial reputation as, in addition to the use cases above, they can also be used to fund various types of attacks on DeFi protocols. Once a vulnerability is uncovered by a malicious actor, the attacker can manipulate certain functions of the protocol using capital acquired via a flash loan and make a profit while potentially draining funds from its smart contracts. In addition, since flash loan transactions revert on failure, hackers don’t have to put a large amount of their own capital at risk to fund an attack.

It’s important to note a key distinction here—flash loans aren’t inherently the problem, since all they do is provide a source of capital. The real issue at hand is existing vulnerabilities in a protocol that may be revealed through a flash loan-funded attack. Over the long-term, flash loans may even be beneficial for the security of the DeFi ecosystem, as protocol engineers have to consider the potential attack vectors flash loans may uncover by providing instant access to a large amount of liquidity.

While attacks often differ in methodology and scope, an attack commonly attributed to flash loans involves manipulating protocols that use a spot price from a [decentralized exchange (DEX)](https://chain.link/education-hub/what-is-decentralized-exchange-dex) as their sole price oracle. As explained in [The Importance of Data Quality for DeFi Smart Contracts](https://blog.chain.link/the-importance-of-data-quality-for-defi/), protocols that fetch prices from a single centralized source are easily exploitable by well-capitalized malicious actors who can manipulate the market with one large trade. DeFi protocols are typically looking to maximize their decentralization and censorship resistance—centralized price oracles undermine this objective by acting as a single point of failure.

Here’s an example of a flash loan-funded attack on a DeFi lending protocol using a DEX-based spot price feed as its sole price oracle:

1. Attacker borrows a large amount of token A from a protocol supporting flash loans.
2. Attacker swaps token A for token B on a DEX (lowering the spot price of token A and increasing the spot price of token B on the DEX).
3. Attacker deposits the purchased token B as collateral on a DeFi protocol that uses the spot price from the above DEX as its sole price feed, and uses the manipulated spot price to borrow a larger amount of token A than should normally be possible.
4. Attacker uses a portion of borrowed token A to fully pay back the original flash loan and keep the remaining tokens, generating a profit using the protocol’s manipulated price feed.
5. As the spot prices of token A and B on the DEX are arbitraged back to the true market-wide price, the DeFi protocol is left with an undercollateralized position.



Steps taken by a malicious actor during a flash loan price oracle attack

Because the attacker was able to open a flash loan and manipulate the exchange that the DeFi protocol used as its sole spot price oracle, the attacker was able to raise the reported value of the token used as collateral and lower the reported value of the token used as debt. This allowed the attacker to borrow more funds than they should have been able to, creating a position that cannot be fully liquidated, as the collateral became worth less than the debt. This attack can occur within a single transaction but can be repeated many times across multiple transactions, furthering the damage.

Furthermore, when used as price feeds,  single on-chain exchanges also provide extremely limited market coverage, as they represent the trading activity of only one exchange. This leaves protocols relying on the spot price from that DEX vulnerable to manipulated price points if volume shifts to different exchanges or a well-capitalized actor temporarily manipulates the price on that exchange. It’s especially risky for lower liquidity assets, which are increasingly being used as collateral within DeFi lending protocols.

With that in mind, this style of attack is entirely preventable with a decentralized [oracle](https://chain.link/education/blockchain-oracles) solution with proper market coverage.

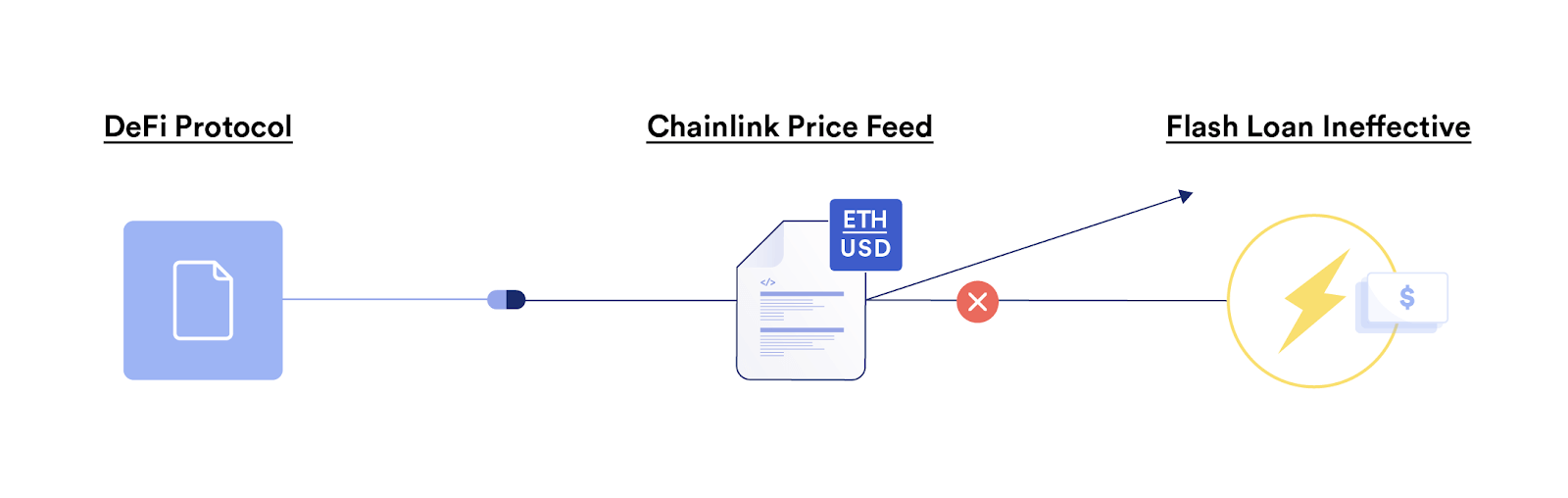
## How Chainlink Oracles Prevent Flash Loan Attacks

In order to generate full market coverage, [Chainlink Price Feeds](https://chain.link/data-feeds) are powered by decentralized networks of nodes that aggregate price data not from a single source but from multiple independent data aggregation firms. These data aggregators track all liquid trading environments—including both centralized and decentralized exchanges—to generate volume-weighted average pricing that reflects the market-wide price of assets. Such data aggregators also commonly take into account various differences between exchanges and actively filter market outliers such as flash crashes and wash trading.

If you’d like a deep dive into the advantages of using Chainlink Price Feeds in DeFi protocols, read [How Chainlink Price Feeds Secure the DeFi Ecosystem](https://blog.chain.link/chainlink-price-feeds-secure-defi/).

Since flash loans only exist within the timeframe of a single on-chain transaction, any manipulation that occurs is reverted by the end of the transaction. Because Chainlink Price Feeds aggregate price data off-chain from a wide collection of sources and publish data on-chain asynchronously, flash loans have no effect on the aggregated values within oracle reports.

To prevent flash loan-related price oracle attacks, it is strongly recommended that smart contract developers avoid manipulatable DEX spot prices and instead utilize Chainlink Price Feeds as their source of validated market data. This helps ensure that DeFi protocols always receive an aggregated price point that is reflective of market-wide trading activity and untouchable by flash loans, mitigating an entire category of price oracle attack vectors.



Flash loans are ineffective against Chainlink Price Feeds.

## Conclusion

Flash loans are a sophisticated financial primitive in DeFi that unlock complex financial applications and lower the barrier to entry for a new wave of market participants. While flash loans have been utilized to fund attacks on DeFi protocols, they are simply a financial tool available to developers and users—they do not create vulnerabilities, but reveal vulnerabilities that may already exist in a protocol, with the most common being faulty price oracle designs.

Chainlink is a decentralized oracle network that helps DeFi protocols become more tamper resistant, particularly regarding the critical function of sourcing real-time market data that will trigger a cascade of other transactions across other [Web3](https://chain.link/education/web3) applications. Only through a [security-first approach](https://blog.chain.link/defi-security-best-practices/) can DeFi protocols adapt to new risks, maintain trust, and sustainably scale to attract billions of users and trillions of dollars of value.

# What Are Stablecoins?

Last Updated Date:

August 14, 2024

DEFINITION

Stablecoins are crypto assets that aim to keep their price “pegged” to the market value of an external asset such as fiat currency or commodity.

While cryptocurrencies are often known for their volatility, stablecoins bring relative stability to cryptocurrency markets by allowing fiat currencies like the U.S. dollar to be represented on the blockchain as digital tokens. These stablecoins allow anyone around the world to hold a token that’s purposely designed to hold its value in relation to the fiat currency it claims to represent (e.g. 1 USD stablecoin tries to maintain a value of 1 U.S. dollar). The desire for stable assets on blockchains has resulted in the wide adoption of stablecoins within the blockchain industry and [decentralized finance (DeFi)](https://chain.link/education/defi).

The explosive growth of total stablecoin supply. ([Source](https://www.theblockcrypto.com/data/decentralized-finance/stablecoins))

‍

In this article, we’ll walk through the fundamental questions around stablecoins—what they are, how they work, and how Chainlink [oracles](https://chain.link/education/blockchain-oracles) power a variety of stablecoin designs.

## What Is a Stablecoin?

At their core, stablecoins are cryptocurrencies that try to maintain a “peg”—the same market value as the external asset they represent. For example, a dollar-based stablecoin will aim to stay pegged to $1, while a gold stablecoin aims to stay pegged to the market price of gold. There are a variety of approaches stablecoins can take to match the price of the currency they’re pegged to consistently, such as collateralization with external assets or algorithmic mechanisms that leverage dynamically adjusting supply in relation to demand.

## Types of Stablecoins

There are two main types of stablecoins: centralized and decentralized.

### Centralized Stablecoins

Centralized stablecoins are traditionally backed by fiat currency in an off-chain bank account that functions as the reserve backing the on-chain tokens. [TrueUSD](https://tusd.io/" \t "_blank) and [USDC](https://www.circle.com/en/usdc) are two examples of centralized stablecoins that employ this method. Alternatively, centralized stablecoins may aim to follow another asset such as a commodity, index, or others. These stablecoin designs typically require trust in the custodian, although [Chainlink Proof of Reserve](https://chain.link/proof-of-reserve) can provide strong transparency guarantees through automated verification.

#### Central Bank Digital Currencies (CBDCs)

Another type of digital asset similar to centralized stablecoins are central bank digital currencies (CBDCs). CBDCs are similar to centralized stablecoins, but they are issued by central banks and thus don’t necessarily have to be backed by fiat money in an off-chain bank account. CBDCs are considered legal tender by the government that issues them and are used for streamlining payments between both individuals and institutions.

### Decentralized Stablecoins

Decentralized stablecoins that employ an overcollateralized design also require a [blockchain price oracle](https://chain.link/education/blockchain-oracles) to help trigger liquidations and ensure protocol solvency. For example, LUSD is an immutable DeFi protocol that enables users to lock up their ETH at a 110% over-collateralization ratio to mint the LUSD stablecoin. [The protocol is underpinned by Chainlink Price Feeds](https://chain.link/case-studies/liquity), which help provide accurate and high-quality price data that the LUSD smart contract uses to automatically trigger liquidations. Another type of decentralized stablecoin—algorithmic stablecoins—typically don’t hold reserves but instead use smart contracts to codify a mechanism to retain their peg with the target index through dynamic supply adjustments or other methods.

## Types of Stablecoin Collateral

Because stablecoins aim to represent assets or commodities that are not natively on-chain, they require collateral to maintain their peg. There are three main types of stablecoin collateral: fiat collateral, digital asset collateral, and commodity collateral.

### Fiat Collateral

Fiat collateral often refers to off-chain fiat currencies such as the dollar, euro, and more. These currencies are held in an off-chain bank account and used to maintain a stablecoin’s peg. This is accomplished through a redemption mechanism—at any point, users can redeem the stablecoin for its off-chain counterpart on a 1:1 basis. For example, users can trade a stablecoin dollar for an off-chain dollar in a bank account, a stablecoin euro for an off-chain euro in a bank account, and so on.

### Digital Asset Collateral

Digital asset collateral refers to the wide range of digital assets that natively exist on blockchain networks. These digital assets are then used as collateral to mint stablecoins, but they require an overcollateralized design to ensure stability—meaning that in order to mint $1 in a stablecoin, a user must put in more than $1 worth of digital asset collateral. This is because digital assets are typically volatile, and it’s imperative that this type of stablecoin protocol is always backed at least 1:1 in value at all times.

### Commodity Collateral

Commodity collateral refers to the many commodities, such as metals, crops, and energy sources, that exist in the world. Like fiat collateral, these commodities exist off-chain, and they require a form of redemption mechanism in order to maintain their peg. To date, the most popular form of commodity collateral has been precious metals like gold, with protocols such as [Cache.gold](https://cache.gold/" \t "_blank) and [Pax Gold](https://paxos.com/paxgold/" \t "_blank) offering users [tokenized gold](https://chain.link/education-hub/tokenized-gold) that can be redeemed for an equivalent amount of gold.

## How Do Stablecoins Work?

There are various economic mechanisms that stablecoins utilize to maintain relative stability by holding their peg. The most common examples of these include the ability to redeem the tokens for fiat money, collateralized debt positions, arbitrage, elastic supply, and more.

### Stablecoin Examples

[USDC](https://www.circle.com/en/usdc) is a centralized stablecoin issued by Circle. Each USDC is backed by one dollar or an asset with equivalent fair value, held in off-chain accounts with regulated financial institutions. Customers with a U.S. dollar bank account can redeem 1 USDC for 1 USD, ensuring that the tokens maintain their 1:1 peg with the U.S. dollar. Other similar centralized stablecoins include USDT, BUSD, TUSD, USDP, and others. Some centralized stablecoins enable the issuer to freeze tokens belonging to a certain address, effectively making the frozen tokens unusable. This method can be used by stablecoin issuers to freeze large amounts of stablecoins obtained through protocol hacks or exploits.

[MakerDAO](https://makerdao.com/en/), a decentralized stablecoin protocol, maintains the peg for its stablecoin, DAI, by having users lock up collateral into a smart contract. The smart contract then mints the stablecoin DAI as overcollateralized debt with an adjustable interest rate. In order to maintain the 1:1 peg of 1 USD = 1 DAI, MakerDAO’s smart contracts adjust the interest rates set by MKR token holders through on-chain governance to encourage borrowers to pay back their debt or take out more stablecoin loans. By encouraging increases or decreases in the total supply via interest rate changes, the price of DAI will change, either rising in value when the supply and interest rate are low or decreasing in value when the supply and interest rate are high.

Another design for decentralized stablecoins involves using arbitrage within a stablecoin index, where the stablecoin is backed by multiple different stablecoins in order to achieve the stability of the peg. For example, if the price of one of the reserve stablecoins exceeds 1 USD while the index price as a whole is below 1 USD, then the smart contract will market sell the stablecoin exceeding 1 USD for the index stablecoin’s token to drive the index price back up to 1 USD. Chainlink oracles can provide reliable and high-quality price feeds that the stablecoin index smart contracts can reference when calculating how to rebalance the index.

‍[Ampleforth (AMPL)](https://www.ampleforth.org/" \t "_blank) is a decentralized, algorithmic stablecoin that uses an elastic supply mechanism to maintain its peg to the current Consumer Price Index (CPI) rate—an index from the Bureau of Economic Analysis on the current value of the inflation-adjusted 2019 U.S. dollar. This effectively means that the price target of AMPL is set to the purchasing power of one 2019 U.S. dollar as represented by the CPI. When the price of AMPL is higher than the index, the protocol increases wallet balances, and when the price of AMPL is lower than the index, the protocol decreases wallet balances. This automated change in supply, referred to as rebasing, impacts market prices by adjusting the outstanding supply of tokens. The total supply of AMPL is rebased on a daily basis to track the CPI rate—both the volume-weighted average price (VWAP) of AMPL and the CPI index are provided to the Ampleforth protocol by Chainlink oracles.

## What Are Stablecoins Used For?

Stablecoins are an integral part of the cryptocurrency and [Web3](https://chain.link/education/web3) ecosystem and account for a significant portion of its trading volume and underlying economic activity.

Stablecoins offer some distinct benefits over their traditional counterparts due to [blockchains](https://chain.link/education-hub/blockchain) being the underlying mechanism facilitating the transfer of value instead of opaque, outdated, and manual processes. Centralized stablecoins effectively allow for value pegged to fiat currencies to move globally between wallets without the need for intermediaries to facilitate the transfer.

Stablecoins are also commonly used as a non-custodial savings account to store personal savings or as collateral in DeFi to generate returns and engage in [yield farming](https://chain.link/education-hub/what-is-yield-farming) strategies.

## Stablecoin Risks

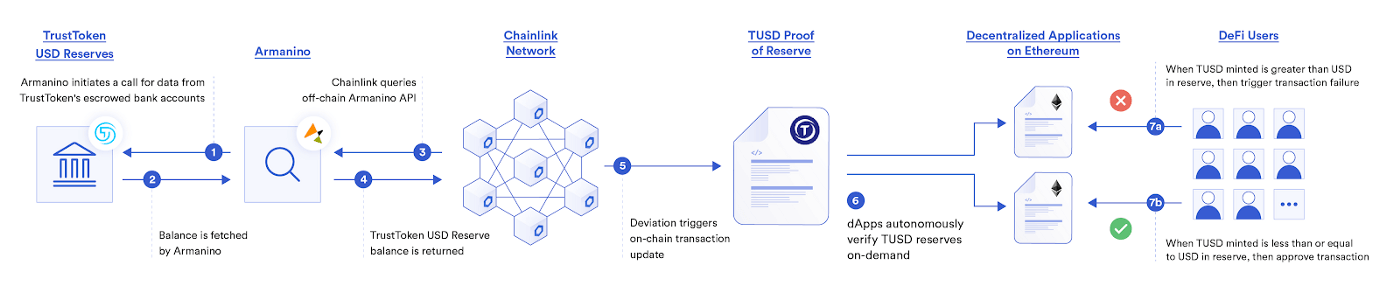
Different stablecoin designs have different risks associated with them. These may include:

* **Depegging risk**—Failure of the underlying economic or algorithmic mechanisms through liquidity events, “bank run” scenarios, suboptimal reserves practices, and more present the risk of the stablecoin depegging from its target.
* **Regulatory risk**—Stablecoins may be regulated in different ways by local financial institutions in particular geographic locations.
* **Centralization risk**—Some centralized stablecoin issuers have the ability to freeze tokens at specific wallet addresses.
* **Key management risk**—If stablecoins are held in a non-custodial wallet, the user must take full responsibility for securely storing their private keys.

Despite the differences in stablecoin architecture, design, and risk, all stablecoins require accurate price data for their underlying pegging mechanism and when used in decentralized applications. Since exchange rates are constantly fluctuating, real-time price data needs to be fed to stablecoins in order for them to maintain their peg. Furthermore, since stablecoins are usually backed by other crypto assets or off-chain bank reserves, tamper-proof methods of acquiring the details of these reserves are needed to ensure the security and reliability of these systems.

[Chainlink](http://chain.link/) is a decentralized oracle network that provides smart contracts with access to a secure and reliable source of real-world data. Since stablecoins collectively hold substantial value in DeFi applications, they require the same assurances and security guarantees as the blockchains they operate on. Effectively, this means that the oracles providing data to stablecoins need to be robust, decentralized, and have [multiple layers of security](https://blog.chain.link/levels-of-data-aggregation-in-chainlink-price-feeds) to help ensure that stablecoin pegs remain at a 1:1 ratio. This provides transparency and trust to the users of these stablecoins, as they can confirm that the stablecoin asset they are using is secure end-to-end and does not contain a single point of failure.

An example of this is [TrueUSD](https://tusd.io/" \t "_blank) (TUSD), which uses Chainlink to bring details of collateralization levels on-chain and give users a clear understanding of whether their assets are fully backed. With this newfound transparency, DeFi users can verify in real-time the reported reserves of all minted TUSD tokens and the protocol itself can automate the protection of users funds from any fractional reserve practices or potential black swan events.

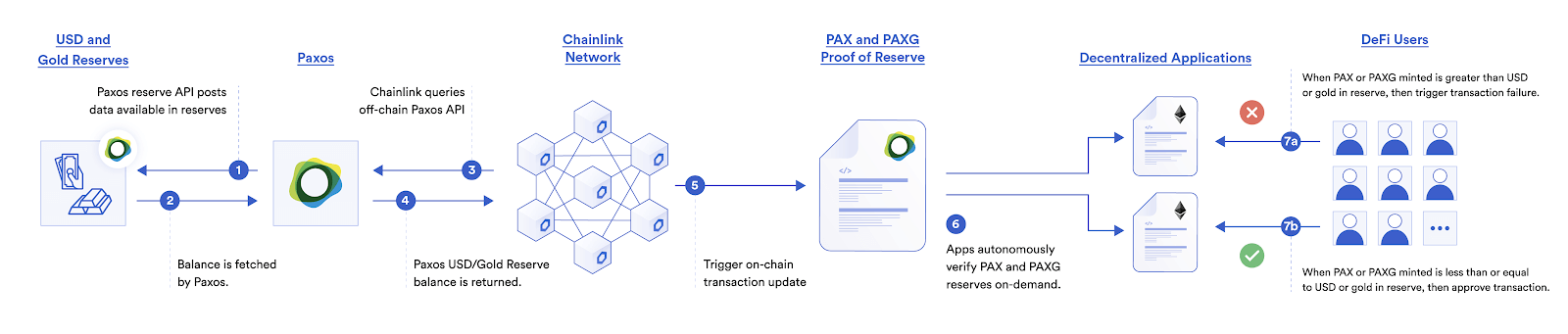


TrustToken uses Chainlink Proof of Reserve to provide smart contracts proof of the off-chain fiat reserves backing the TUSD stablecoin.

This mechanism for verifying the reserves of an asset leverages Chainlink Proof of Reserve (PoR). PoR reference feeds provide smart contracts with the data needed to calculate the true collateralization of any on-chain asset backed by off-chain reserves. These reference feeds are operated by a decentralized network of oracles on the Chainlink Network and allow for the autonomous auditing of collateral used within a protocol in real-time, helping ensure that user funds are protected from unforeseen fractional reserve practices and other fraudulent activity from off-chain custodians.

For stablecoin protocols that utilize off-chain reserves, recurring audits enabled by Chainlink PoR help enhance transparency and ensure the status of the reserves backing a stablecoin. Stablecoins that use PoR can offer a higher degree of transparency to their users as they can prove that their tokens are backed. PoR can also provide collateralization data regarding any type of pegged asset, including alternative fiat currencies or commodities like gold, increasing the transparency of any token protocol utilizing this mechanism.

‍[Paxos](https://paxos.com/2021/01/14/paxos-adopts-chainlink-oracles-to-further-adoption-of-pax-and-paxg-in-defi/" \t "_blank), a financial market infrastructure and crypto brokerage platform, uses Chainlink to provide DeFi smart contracts with a highly available, tamper-proof, and accurate source of on-chain pricing data for the USD-backed stablecoin Pax Dolar (USDP) and the gold-backed token PAX Gold (PAXG). Additionally, Chainlink [Proof of Reserve Data Feeds for Paxos tokens](https://data.chain.link/ethereum/mainnet/reserves/paxg-reserves) allow DeFi applications to quickly verify on-chain that tokens are fully backed 1:1 by U.S. dollars and gold bars held off-chain in Paxos’ custody.



How Paxos uses Chainlink Proof of Reserve to verify the collateralization of off-chain assets.

Central Bank Digital Currencies (CBDCs) will likely also be pegged to an external asset, meaning that they would need to be able to receive price data about that asset. Chainlink could support these government-issued stablecoins by providing the price data needed for them to maintain their pegs along with important information about the current collateralization of the system.

## Why Stablecoins Are Important

Stablecoins are a key innovation that pioneered a now increasingly important subset of the Web3 ecosystem known as [tokenized real-world assets](https://chain.link/education-hub/asset-tokenization) (RWAs)—or the tokenization of assets that society today uses on a daily basis. They are an early indicator of the benefits and efficiencies that mass adoption of digital assets can bring.

For example, the most widely adopted stablecoins are dollar-pegged digital assets that effectively act as on-chain representations of the dollar. These stablecoins are leveraged by Web3 users around the world to build an on-chain savings account, protect against market volatility, leverage as a medium of exchange, earn yield, or send money across the globe. Given the [$100B+ market cap](https://www.theblock.co/data/decentralized-finance/stablecoins) for stablecoins, it’s crystal clear that Web3 users desire the stability that stablecoins offer.

## Conclusion

Despite their simplicity, stablecoins can be considered to be one of the cryptocurrency industry’s most significant innovations, allowing for the seamless transfer of stable value. While there are a number of different stablecoin designs, the common backbone of any stablecoin protocol is the data that it receives about the asset it is pegged to. Chainlink provides the battle-tested data infrastructure that helps ensure the reliability, security, and transparency of stablecoins and the stability of the larger DeFi ecosystem.

If you’re a developer and want to integrate Chainlink into your smart contract applications, check out the [developer documentation](https://docs.chain.link/) or [reach out to an expert](https://chain.link/contact?ref_id=education_hub).

**What Is a DEX (Decentralized Exchange)?**

Last Updated Date:

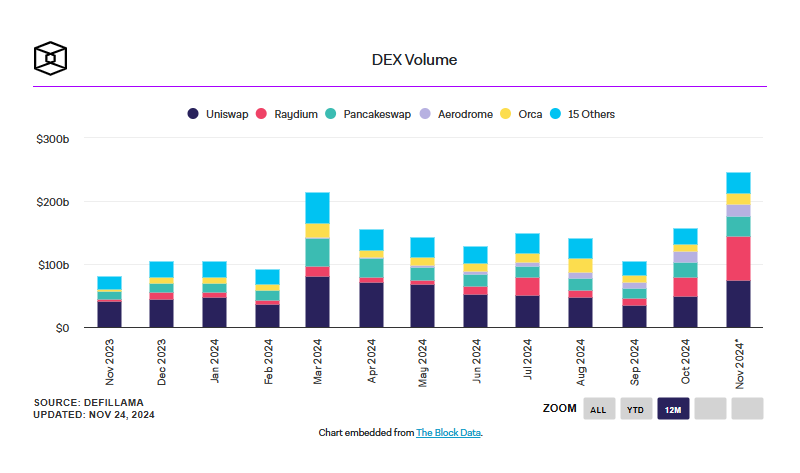
August 14, 2024

DEFINITION

A decentralized exchange (DEX) enables users to trade crypto assets through blockchain transactions without the need for a custodian or centralized intermediary.

**A DEX (decentralized exchange) is a peer-to-peer marketplace where users can trade cryptocurrencies in a non-custodial manner without the need for an intermediary to facilitate the transfer and custody of funds.** DEXs substitute intermediaries—traditionally, banks, brokers, payment processors, or other institutions—with blockchain-based [smart contracts](https://chain.link/education/smart-contracts) that facilitate the exchange of assets.

Compared to traditional financial transactions, which are opaque and run through intermediaries who offer extremely limited insight into their actions, DEXs offer complete transparency into the movement of funds and the mechanisms facilitating exchange. In addition, as user funds don’t pass through a third party’s cryptocurrency wallet during trading, DEXs reduce counterparty risk and can decrease systemic centralization risks in the cryptocurrency ecosystem.

DEXs are a cornerstone of [decentralized finance (DeFi)](https://chain.link/education/defi) and serve as a key “money LEGO” upon which more sophisticated financial products can be built as a result of [permissionless composability](https://chain.link/education-hub/permissionless-composability).  


*The swift growth of DEX spot volume. (*[*Source*](https://www.theblockcrypto.com/data/decentralized-finance/dex-non-custodial/dex-volume-monthly)*)*

This article outlines how decentralized exchanges work, the different types of DEX, and the benefits and risks they bring to the cryptocurrency ecosystem.

**How Does a DEX Work?**

There are several DEX designs, each offering a different benefits and trade-offs in terms of feature-sets, scalability, and decentralization. The two most common types are order book DEXs and [automated market makers (AMMs)](https://chain.link/education-hub/what-is-an-automated-market-maker-amm). DEX aggregators, which parse through multiple DEXs on-chain to find the best price or lowest gas cost for the user’s desired transaction, are also a widely used category.

One of the main benefits of DEXs is the high degree of determinism achieved by using [blockchain technology](https://chain.link/education-hub/blockchain) and immutable smart contracts. Whereas in centralized exchanges (CEXs), such as Coinbase or Binance, the platform facilitates trading using the internal matching engine of the exchange, DEXs execute trades through smart contracts and on-chain transactions. Furthermore, DEXs allow users to maintain full custody of their funds via their self-hosted wallets during trading.

DEX users are typically required to pay two types of fees—network fees and trading fees. Network fees refer to the gas cost of the on-chain transaction while trading fees are collected by the underlying protocol, its liquidity providers, token holders, or a combination of these entities as specified by the design of the protocol.

The vision behind many DEXs is to have permissionlessly accessible, end-to-end on-chain infrastructure with no central points of failure and decentralized ownership across a community of distributed stakeholders. This typically means protocol administrative rights are governed by a decentralized autonomous organization (DAO), made up of a community of stakeholders, which votes on key protocol decisions.

However, maximizing the decentralization of the protocol while keeping it competitive in a crowded DEX landscape isn’t an easy feat, as the core development team behind the DEX is generally able to make more informed decisions about mission-critical protocol functionality than a distributed set of stakeholders. Even so, many DEXs opt for a [distributed governance](https://blog.chain.link/how-chainlink-powers-decentralized-governance/) structure in an attempt to increase censorship resistance and long-term resiliency.

**Order Book DEXs**

An order book—a real-time collection of open buy and sell orders in a market—is a foundational pillar of electronic exchanges. Order books allow an exchange’s internal systems to match buy and sell orders.

Fully on-chain order book DEXs have been historically less common in DeFi, as they require every interaction within the order book to be posted on the blockchain. This requires either far higher throughput than most current blockchains can handle or significant compromises in network security and decentralization. As such, early examples of order book DEXs on Ethereum had low liquidity and suboptimal user experience. Even so, these exchanges were a compelling proof of concept for how a DEX could facilitate trading using smart contracts.

With scalability innovations such as layer-2 networks like optimistic rollups and ZK-rollups and the launch of higher-throughput and app-specific blockchains, on-chain order book exchanges have become more feasible and now attract a considerable amount of trading activity. Additionally, hybrid order book designs have become more popular, where the order book management and matching processes take place off-chain while the settlement of trades occurs on-chain.

Some popular order book DEXs include 0x, dYdX, Loopring DEX, and Serum.

**Automated Market Makers (AMMs)**

Automated market makers are the most widely used type of DEX as they enable instant liquidity, democratized access to liquidity provision, and—in many cases—permissionless market creation for any token. An AMM is essentially a money robot that is always willing to quote a price between two (or more) assets. Instead of an order book, an AMM utilizes a liquidity pool that users can swap their tokens against, with the price determined by an algorithm based on the proportion of tokens in the pool.

Since they’re always able to quote a price for a user, AMMs enable instant access to liquidity in markets that otherwise may have lower liquidity. In the case of an order book DEX, a willing buyer has to wait for their order to be matched with the order of a seller—even if the buyer posts their order to the “top” of the order book close to the current price, the order may never execute.

In the case of an AMM, the exchange rate is determined by a smart contract. Users can get instant access to liquidity, while liquidity providers (depositors into the AMM’s liquidity pool) can earn passive income via trading fees. This combination of instant liquidity and democratized access to liquidity provision has enabled an explosion of new tokens being launched through AMMs and unlocked new designs that focus on distinct use cases, such as [stablecoin](https://chain.link/education-hub/stablecoins) swaps. If you’d like a more detailed exploration of AMMs, read this post covering [how AMMs work](https://chain.link/education-hub/what-is-an-automated-market-maker-amm).

While most current AMM designs deal with cryptocurrencies, AMMs could also be used to facilitate swaps of [NFTs](https://chain.link/education/nfts), [tokenized real-world assets](https://blog.chain.link/real-world-assets-rwas-explained/), carbon credits, and much more.

Some popular AMM DEXs include Bancor, Balancer, Curve, PancakeSwap, Sushiswap, Trader Joe, and Uniswap.

**What Are the Benefits of Decentralized Exchanges?**

Since DEX trades are facilitated by deterministic smart contracts, they carry strong guarantees that they will execute in exactly the manner the user intended, without the intervention of centralized parties. In contrast to the opaque execution methods and potential for censorship present in traditional financial markets, DEXs offer strong execution guarantees and increased transparency into the underlying mechanics of trading.

In this video, Sergey Nazarov, co-founder of Chainlink, discusses how the need for cryptographically enforced guarantees is increasing the demand for decentralized infrastructure:

As there are no custodians involved and users can participate using their self-hosted wallets, DEXs reduce counterparty risk. DEXs can also reduce some of the systemic risks of the blockchain industry by reducing the amount of capital concentrated in the wallets of a small number of centralized exchanges. In 2014, the Mt. Gox centralized exchange handled a significant portion of all Bitcoin trading volume before it abruptly ceased operations amid the loss of hundreds of thousands of bitcoin.

DEXs also help increase financial inclusion. While there have been cases of specific user interfaces limiting access based on geographic location or other factors, accessing a DEX’s smart contracts only requires an Internet connection and a compatible self-hosted wallet. As users are able to sign in in a straightforward manner using their wallet address, the onboarding process for a DEX is seamless and practically instantaneous compared to a centralized exchange.

**DEX Risks and Considerations**

DEXs have democratized access to trading and liquidity provision through strong execution guarantees, increased transparency, and permissionless access. However, DEXs also carry a set of risks, which include but are not limited to:

* Smart contract risk—Blockchains are considered highly secure for executing financial transactions. However, the code quality of a smart contract is nevertheless dependent on the skill level and experience of team that developed it. Smart contract bugs, hacks, vulnerabilities, and exploits can occur, leaving DEX users susceptible to a loss of funds. Developers can mitigate this risk through security audits, peer-reviewed code, and sound testing practices, but diligence is always required.
* Liquidity risk—While DEXs are becoming increasingly popular, some DEX markets have poor liquidity conditions, leading to large amounts of slippage and a suboptimal user experience. Due to how the network effects of liquidity works (high liquidity attracts more liquidity, low liquidity attracts less liquidity), significant portions of trading activity is still conducted on centralized exchanges, which often leads to less liquidity on DEX trading pairs.
* Frontrunning risk—Due to the public nature of blockchain transactions, DEX trades may be frontrun by arbitrageurs or [maximal extractable value (MEV)](https://blog.chain.link/maximal-extractable-value-mev/) bots trying to siphon value from unwitting users. Similar to high-frequency traders in traditional markets, these bots try to exploit market inefficiencies by paying higher transaction fees and optimizing network latency to exploit ordinary users’ DEX trades.
* Centralization risk—While many DEXs aim to maximize their decentralization and censorship resistance, points of centralization can still be present. These include the DEX’s matching engine being hosted on centralized servers, the development team having administrative access to the DEX’s smart contracts, and the use of low-quality token bridging infrastructure among others.
* Network risk—As the exchange of assets is facilitated by a blockchain, using a DEX may be prohibitively expensive or outright impossible if the network experiences congestion or downtime, leaving DEX users susceptible to market movements.
* Token risk—As many DEXs feature permissionless market creation—the ability for anyone to create a market for any token—the risks of buying low-quality or malicious tokens can be higher than in centralized exchanges. DEX users need to consider the risks associated with participating in early-stage projects.

In addition to the above, some users may find having full custody of their private keys a daunting prospect. While having full control over one’s assets is one of the main benefits offered by the [Web3](https://chain.link/education/web3) vision, many users may prefer to have a third party entrusted with the custody of their assets. However, following good [security](https://blog.chain.link/defi-security-best-practices/) and key management practices can allow more users to enjoy the benefits of maintaining full control over their assets while accessing a sophisticated ecosystem of open-source financial services.

**How DEXs Can Use Chainlink To Help Increase Security and Unlock Advanced Features**

DEXs can use Chainlink [oracle](https://chain.link/education/blockchain-oracles) services to increase the resiliency of their protocol and introduce advanced features that users may be familiar with from centralized infrastructure.

[Chainlink Price Feeds](https://data.chain.link/) provide accurate, secure, and reliable financial market data on cryptocurrencies, commodities, forex, indices, and more, and help secure tens of billions of dollars for DeFi applications across the multi-chain ecosystem. Using Chainlink decentralized oracle networks, dApps are able to retrieve off-chain price data in a simple, secure, and decentralized manner and execute actions based on that data.

DEX protocols can use Chainlink Price Feeds for reliable price conversions, accurate display prices on a frontend, or the secure calculation of [staking](https://chain.link/education-hub/what-is-staking-crypto) rewards and fee distributions to stakeholders. On DEXs involving margin or futures contracts, Price Feeds can help ensure the correct pricing of collateral assets and the accurate processing of liquidations.

Chainlink Price Feeds can also be used as an additional backstop by DEXs looking to increase the resilience of their protocol to outlier market events, which a battle-tested source of price data can help protect against. Secure price infrastructure can also help ensure the security and accuracy of price monitoring and financial analysis infrastructure, and help create and manage arbitrage strategies between different decentralized exchanges.

[Chainlink Automation](https://chain.link/automation), a decentralized automation solution, is also widely used in the DeFi ecosystem to support the introduction of sophisticated features through end-to-end [smart contract automation](https://chain.link/education-hub/smart-contract-automation). Chainlink Automation uses decentralized and reliable off-chain computation to monitor user-defined conditions and then call on-chain functions once those conditions are satisfied.

Chainlink Automation can trigger limit orders when asset prices cross predefined price points, empowering traders to have more granular control of their portfolios and saving development teams time and resources that they can then spend improving the core business logic of their protocol. Chainlink Automation can also be used to reliably perform the periodic distribution of trading fees and staking rewards.

**Conclusion**

DEXs are a foundational pillar of the cryptocurrency ecosystem, letting users exchange digital assets in a peer-to-peer manner without the need for intermediaries. DEXs have experienced increasing adoption in the last few years due to the instant liquidity they can enable for newly launched tokens, their seamless onboarding experience, and the democratized access to trading and liquidity provision they provide.

It remains to be seen if the majority of trading activity will migrate to DEXs and whether current DEX designs will support long-term growth and [institutional adoption](https://blog.chain.link/chainlink-enterprise-blockchain-middleware/). However, DEXs are expected to remain vital infrastructure for the cryptocurrency ecosystem and will continue to see improvements in transaction scalability, smart contract security, governance infrastructure, and user experience.

If you are a DeFi developer and want to integrate Chainlink, check out our [documentation](https://docs.chain.link/), ask a question in [Discord](https://discord.com/invite/aSK4zew), or [set up a call](https://chain.link/contact?ref_id=education_hub) with an expert.

# What Is a Decentralized Money Market?

Last Updated Date:

August 14, 2024

DEFINITION

Decentralized money markets enable users to borrow and lend on-chain digital assets with just an Internet connection.

One of the most fundamental mechanisms of a healthy economy is the ability to put idle capital to work, enabling people to borrow money to grow their businesses and pay for expenses, and enabling others to lend assets to earn yield and grow their savings. In order to meet these needs, money markets—venues that connect borrowers and lenders—were created to meet this demand and over the centuries have generated significant economic activity.

While money markets have changed over time, their purpose and fundamental design remains largely the same. Borrowers use money markets to take out a short term loan (typically under a year) in order to borrow one currency (e.g. dollars), while putting up another currency (e.g. Euros) or an asset (e.g. real estate) as collateral. This collateral is required in the event the borrower fails to pay back their debts, in which case the collateral is sold to make the lender whole. Otherwise the collateral is returned when the loan is paid off by the borrower.

In exchange for the ability to borrow working capital from lenders, borrowers are required to pay a fee, usually in the form of an annual interest rate (e.g. 7% a year), which generates yield for lenders and incentives deposits. This interest rate is typically a function of supply and demand to ensure sufficient liquidity is available to both borrowers and lenders. A high supply and low demand of an asset leads to lower interest rates, while low supply and high demand of an asset leads to a higher interest rate. Various money markets compete based on the interest rates they offer, as well as other parameters such as how much collateral is required for loans.

With the rise of the [Decentralized Finance (DeFi)](https://chain.link/education/defi) ecosystem, decentralized money market protocols like [Aave](http://aave.com/" \t "_blank) and [CREAM](http://cream.finance/) enable users to borrow and lend their on-chain cryptocurrency (and [tokenized assets](https://blog.chain.link/definitive-guide-to-tokenized-assets/)) with just an internet connection. Today, billions of user funds are flowing through these on-chain money markets, which have been a rapidly growing use case of smart contracts alongside the growth of DeFi as a whole. However, to truly understand the benefits of decentralized money markets, it is key to examine the benefits they bring over traditional lending and borrowing venues.

## The Benefits of Decentralized Money Markets

While traditional money markets have been a net positive for the global economy over the centuries, enabling business to expand and allowing citizens to save their money, the money markets of today are typically operated by a centralized institution, granting a significant amount of power and influence over user funds to a single entity. This design increases costs for borrowers/lenders and requires a high degree of trust in a single party.

In response to these limitations, developers are now utilizing blockchain-based [smart contracts](https://chain.link/education/smart-contracts) to create decentralized money markets that operate as code on a highly decentralized network of nodes around the world. Instead of being operated by a centralized institution, decentralized money markets are operated through on-chain programmatic code that is upgraded and managed by a global community of stakeholders, decentralizing control and reducing points of failure. Below represent a few of the primary advantages decentralized money markets bring to consumers.

### Non-custodial

Decentralized money markets operate in a non-custodial manner where deposited funds from borrowers and lenders can only be withdrawn by the original user themselves. Instead of a centralized institution deciding where and how funds are used, decentralized money markets follow predefined logic of on-chain smart contracts, granting a large degree of assurance that funds cannot be improperly used and ensuring that users keep full control over when and how they can withdraw.

### Permissionless

Through these smart contracts, on-chain money markets are also able to operate in an inherently permissionless manner where users do not need to ask permission from a central gatekeeper. This enables anyone with access to the internet to earn yield and/or borrow working capital with minimal friction. This censorship-resistance creates a wider market of users, including the underbanked, generating more economic activity and higher yields as a result.

### Overcollateralized

Unlike the traditional financial system which commonly operates in an undercollateralized and fractional reserve manner where users can borrow more funds they deposit as collateral, decentralized money markets operate in an overcollateralized manner. By depositing more collateral than what is being borrowed, borrowers who are unable to pay back their debts simply have their collateral liquidated, providing a high degree of security for lenders.

### Open composability

Smart contract powered financial applications like decentralized money markets have the unique advantage that deposited funds can be tokenized (e.g. tokens deposited on Aave becomes fungible aTokens). These tokenized deposits become interest-bearing representations of the underlying assets and can then be used within other applications within the decentralized finance ecosystem. This creates what is known as [composability](https://chain.link/education-hub/permissionless-composability) and allows for the creation of more advanced applications such as no-loss lotteries like [PoolTogether](http://pooltogether.com/" \t "_blank), where user funds are pooled in a money market to generate interest which is then distributed to one winner a week, while all users can withdraw their full original deposit at any time.

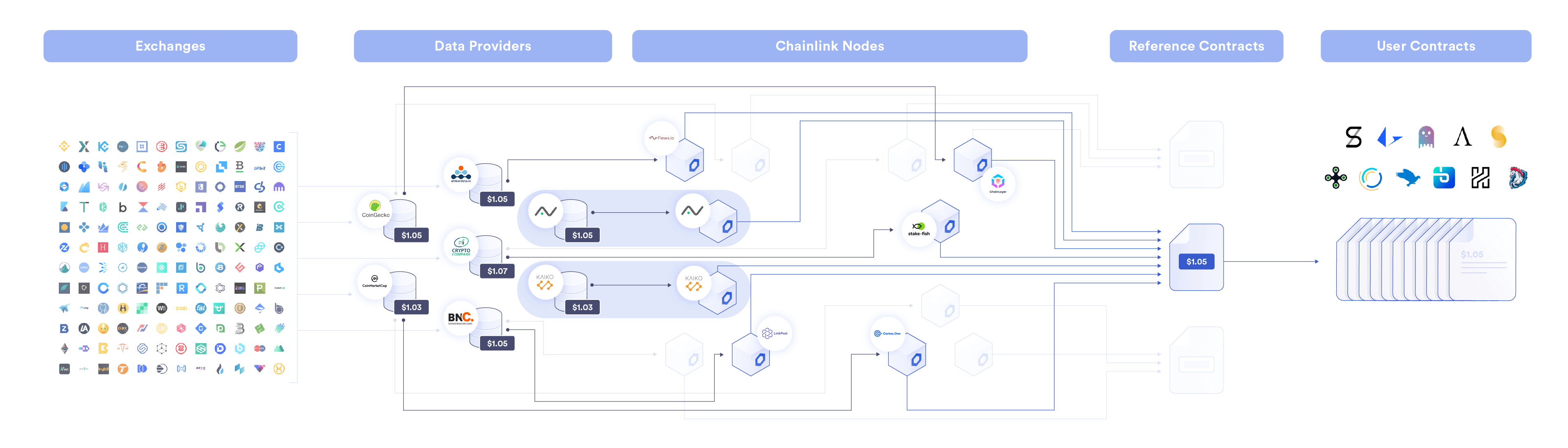
With all of these advantages in combination, decentralized money markets have become one of the most widely used applications in the DeFi economy alongside decentralized exchanges and [stablecoins](https://chain.link/education-hub/stablecoins). However, beyond the on-chain smart contract logic itself, decentralized money markets also need an additional piece of core infrastructure in order to function properly.

## The Importance of Price Feeds for Decentralized Money Markets

To ensure decentralized money markets stay overcollateralized and do not become insolvent, they require real-time price data on each supported asset on the exchange. This price data is used to determine when borrowers should have their position liquidated—where collateral is sold to liquidators who pay back the user’s debt for a fee—which can occur if the collateral falls in value and/or the debt rises in value.

However, because of the [blockchain oracle problem](https://blog.chain.link/what-is-the-blockchain-oracle-problem/), smart contracts cannot natively access off-chain information such as price data, necessitating the usage of an oracle to relay this data on-chain. If a decentralized money market utilizes an insecure oracle mechanism that only provides low quality data, then user funds can be at risk of loss. As an example, if the price oracle deviates below the market wide price, borrowers can become falsely liquidated, and if the price oracle deviates above the market wide price, then users can create undercollateralized toxic positions on the protocol. Because liquidations play such a crucial role in ensuring the health of decentralized money markets, it is imperative pricing data is received from a [highly secure oracle mechanism](https://chain.link/education-hub/flash-loans).

As the most widely used decentralized oracle solution, [Chainlink Data Feeds](https://chain.link/data-feeds) provide numerous on-chain money markets, such as [Aave](https://medium.com/aave/the-aave-oracle-network-powered-by-chainlink-is-now-live-45bb8a5a8c4e" \t "_blank) and [CREAM](https://medium.com/cream-finance/c-r-e-a-m-finance-affirms-chainlink-as-our-primary-price-oracle-solution-7d2d286b6fb9), with a highly secure and reliable source of price data on a multitude of crypto assets. Chainlink mitigates any single point of failure by being decentralized at both the node operator and data source levels, with quality control measures in place to ensure a consistently high level of manipulation resistance. Additionally, Chainlink Price Feeds are able to ensure money markets receive price data with full market coverage by fetching from multiple professional data aggregators that each track all trading venues, taking into account volume, liquidity, and time differences across exchanges.



Chainlink Price Feeds have multiple layers of aggregation for tamper-resistance

Through Chainlink’s time-tested and battle-hardened Price Reference Data Feeds, communities managing decentralized money markets can invest their resources in onboarding new collateral types and ensuring a healthy protocol. Chainlink’s [oracle](https://chain.link/education/blockchain-oracles) framework guarantees that these markets source pricing information that will continue to operate as designed, with the additional ability to rapidly launch new feeds as needed. Using this approach, decentralized money markets such as Aave, which now secures over a billion in deposited funds, has been able to rapidly expand and include new unique collateral types such as real-world mortgages and [decentralized exchange](https://chain.link/education-hub/what-is-decentralized-exchange-dex) liquidity pool tokens.

## Conclusion

Decentralized money markets provide the DeFi ecosystem with a crucial building block on which advanced financial products can be built. While lending and borrowing is useful on its own, it becomes even more powerful when combined with other DeFi “money legos” to create a sum greater than its parts. As these money markets expand, they will not only grow in liquidity and provide more utility and opportunity for more users, but they will also be the forefront of innovation in DeFi as yields in the real-world economy become increasingly unpredictable. The future for decentralized money markets is brighter than ever.

# What Are Proof of Reserves?

DEFINITION

Proof of Reserves (PoR) verifies digital asset collateralization held by crypto businesses, helping bring greater transparency to depositors via public reserves reporting or independent audits.

The global financial system commonly operates in an undercollateralized and highly opaque manner, creating systemic risks that can result in boom and bust cycles and market-wide failures. [Decentralized finance (DeFi)](https://chain.link/education/defi) provides an alternative by offering highly transparent, trust-minimized financial products that are powered by deterministic smart contracts and [cryptographic truth](https://blog.chain.link/what-is-cryptographic-truth/). With the growth of DeFi comes an increasing demand for new collateral types that extend beyond native on-chain assets, including cross-chain tokens, fiat-backed stablecoins, tokenized real-world assets, and more.

In this article, we’ll break down what Chainlink Proof of Reserve (PoR) is and how it helps provide stronger security guarantees and more transparency in the cryptocurrency ecosystem. In addition, we’ll also explore the PoR reference feeds already implemented by top DeFi teams and provide context for future use cases and implementations.

## What Is Proof of Reserve?

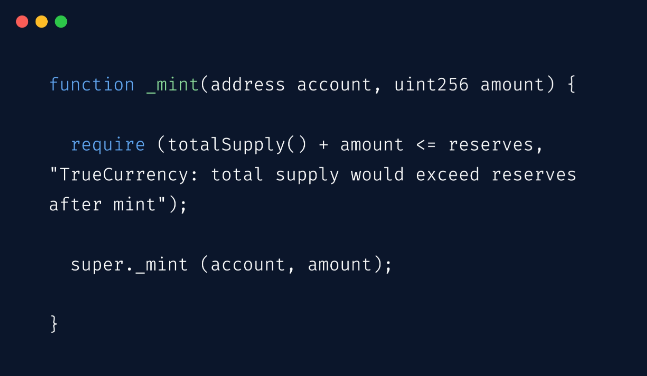
Proof of Reserve traditionally refers to businesses that hold cryptocurrency creating public reports regarding their reserves to prove their solvency to their depositors via an independent audit. As these audits are commonly done by a centralized third party, they can be lengthy, time-consuming, and require manual processes.

As developers continue to build increasingly sophisticated financial products in the digital asset ecosystem, a reliable, transparent, and decentralized standard is required to enable reserves to be audited using an automated process leveraging the superior transparency of blockchains, [smart contracts](https://chain.link/education/smart-contracts), and oracles—enter Chainlink PoR.

## Chainlink Proof of Reserve (PoR)

[Chainlink Proof of Reserve](https://chain.link/proof-of-reserve) provides smart contracts with the data needed to calculate the true collateralization of any on-chain asset backed by off-chain or cross-chain reserves. Operated by a decentralized network of [oracles](https://chain.link/education/blockchain-oracles), Chainlink Proof of Reserve enables the autonomous auditing of collateral in real-time, helping ensure user funds are protected from unforeseen fractional reserve practices and other fraudulent activity from off-chain custodians. Rather than forcing users to trust paper guarantees made by custodians, Chainlink PoR can be deployed for automated on-chain audits that give users a superior guarantee of an asset’s underlying collateralization and generate a higher degree of transparency for the crypto asset ecosystem around asset collateralization.

Chainlink PoR Secure Mint enhances stablecoin and tokenized asset security by providing cryptographic guarantees that new tokens minted are backed by reserves, helping to prevent infinite mint attacks. Asset tokenization projects such as [TUSD](https://trueusd.medium.com/trueusd-becomes-first-usd-backed-stablecoin-to-secure-minting-with-proof-of-reserves-fe8dbffde44f), [PoundToken](https://chain.link/case-studies/poundtoken), and [Cache Gold](https://chain.link/case-studies/cache-gold) have integrated PoR Secure Mint to employ this standard for tokenized asset transparency, security, and verifiability.



Furthermore, Chainlink PoR is also increasingly being used to help secure the minting, redeeming, and burning of wrapped assets. Once Chainlink PoR determines that wrapped tokens are undercollateralized, [Chainlink Automation](https://chain.link/automation) can be used to halt the minting, redeeming, and burning of wrapped tokens.

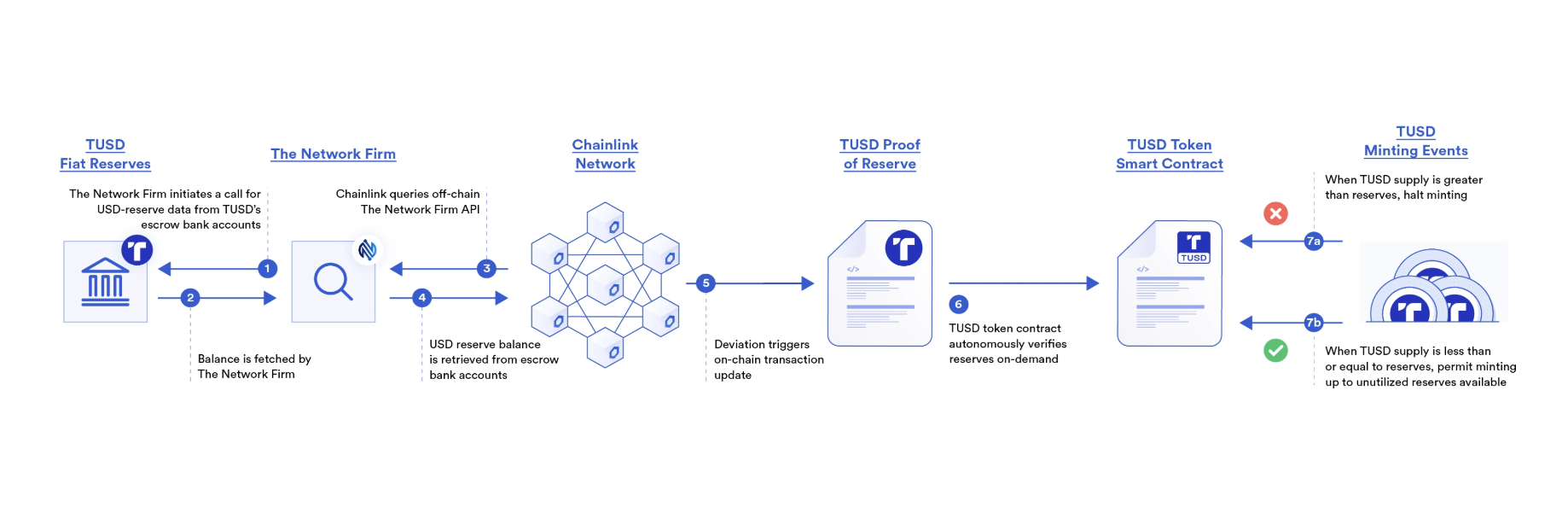
## Proof of Reserve for Off-Chain Assets

[Stablecoins](https://blog.chain.link/what-are-stablecoins/) are a key building block within the DeFi ecosystem, providing users with the ability to transact and earn yield in a comparatively low-volatility currency while still benefiting from the deterministic nature of smart contracts. As such, stablecoins are a popular collateral choice and are fundamental to scaling the adoption of DeFi products.

With more than a hundred billion dollars of value in the stablecoin ecosystem, it is becoming increasingly important to provide smart contracts with proof that each collateralized stablecoin is fully backed by an equal amount of value in an off-chain bank account.

By leveraging data generated by professional auditors, Chainlink PoR provides smart contract applications with collateralization data regarding the off-chain reserves of fiat-backed stablecoins. As an example, the TUSD Reserves provides DeFi users and applications with data regarding the reported offchain reserves for TUSD, as well as the supply of TUSD tokens minted across multiple blockchains.

To power the TUSD Proof of Reserve reference feed, Chainlink oracles fetch data from The Network Firm, which performs regular reviews of TrustToken’s escrowed bank accounts. When the amount of US dollars held in TrustToken’s reserves deviates beyond a predefined threshold, an update is pushed on-chain to the Proof of Reserve reference feed. DeFi applications can then utilize this data to verify the reserves of TUSD tokens on-demand.



Chainlink Proof of Reserve provides smart contracts proof regarding the amount of US dollars backing TrustToken’s stablecoin TUSD.

TUSD uses Chainlink PoR in an additional way—to add even more enhanced security and transparency to the stablecoin minting process. Chainlink Proof of Reserve Secure Mint enables stablecoin issuers to programmatically require reserves to be greater than or equal to the supply being minted. By providing cryptographic guarantees that new tokens minted are backed by reserves, PoR Secure Mint takes tokenized asset and stablecoin security to the next level, helping to prevent infinite mint attacks.

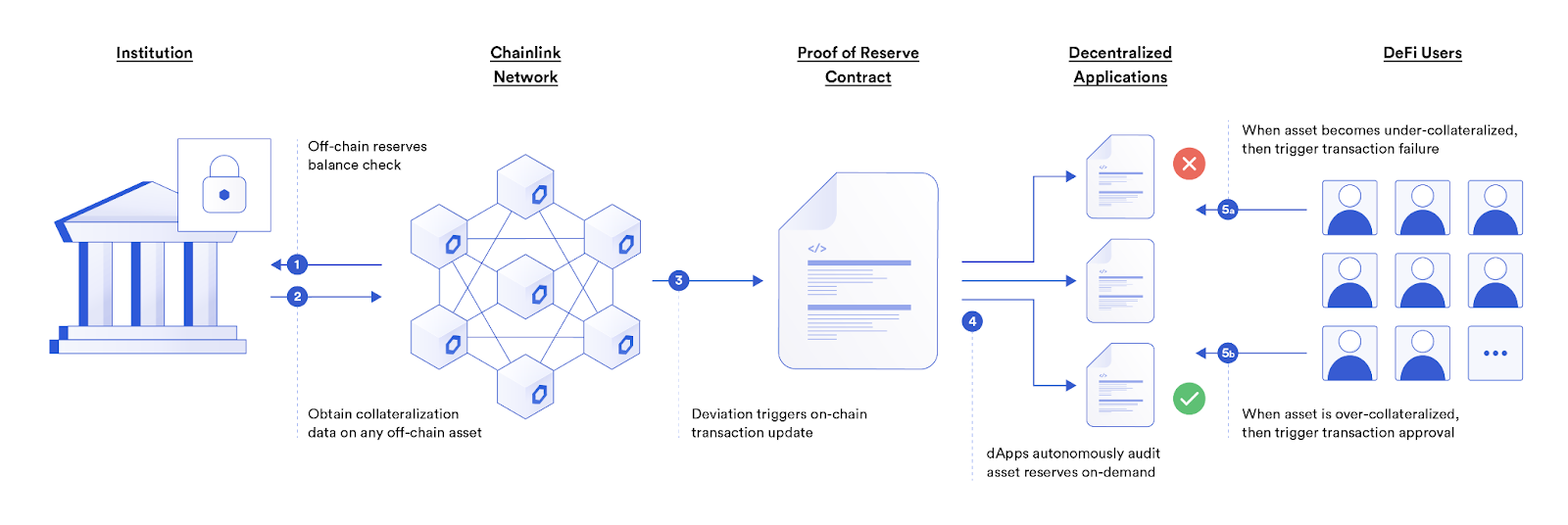
Secure Mint is being integrated by stablecoins, such as [Poundtoken](https://chain.link/case-studies/poundtoken), and tokenized assets, such as Cache Gold, in their minting smart contract to help ensure reserves are sufficient before minting new tokens.

Following this model, Proof of Reserve reference feeds can be deployed to track the collateralization and secure the minting of any stablecoin backed by off-chain fiat reserves. Through this data, the economic activity of stablecoins can accelerate within DeFi not only from retail users but also from traditional institutions that are seeking to securely generate yield in the decentralized finance ecosystem.

Beyond USD-backed stablecoins—which are the most popular pegged assets within the DeFi ecosystem—Chainlink Proof of Reserve feeds can also be constructed to provide collateralization data regarding any type of pegged asset. These can include fiat currencies such as GBP or commodities like gold, increasing the transparency of an entire category of building blocks within DeFi.

## Proof of Reserve in Traditional Markets And Tokenized Real-World Assets

While current implementations provide transparency on the collateralization of tokens that are currently used within the cryptocurrency ecosystem, the Chainlink Proof of Reserve model is much broader in scope and can be utilized to bring transparency to the growing asset tokenization market. Tokenized assets that previously required an impractical level of trust in the issuer are now able to utilize Proof of Reserve to provide the transparency required for user adoption.



How Chainlink PoR helps secure wrapped tokens backed by off-chain reserves.

Chainlink PoR feeds can be used for a wide range of [tokenized real-world assets (RWAs)](https://blog.chain.link/tokenized-real-world-assets/), such as real estate properties that generate verifiable cash flows. Both the ownership of the property and the escrowed bank account holding the USD cash flows generated are able to be audited and brought on-chain, enabling smart contracts to mint trust-minimized tokenized representations of both the real estate property and its cash flow, with collateralization verified by a decentralized network of Chainlink oracles. Chainlink PoR can also be used to support the tokenization of other types of RWAs, such as commodities like gold and silver. Paxos and CACHE Gold are using Chainlink PoR to enable anyone to quickly verify on-chain that their [tokenized gold](https://chain.link/education-hub/tokenized-gold) products are fully backed by gold reserves held in off-chain custody.

Furthermore, Proof of Reserve feeds can be used beyond the world of DeFi and smart contract applications. For example, they can provide traditional financial institutions with a way to increase trust with customers and counterparties by using Chainlink oracles to publish their audit reports on-chain as an immutable and tamper-proof record.

By leveraging blockchain technology without any modifications to their business model or [backend enterprise systems](https://blog.chain.link/chainlink-enterprise-blockchain-middleware/), institutions can provide a definitive and immutable source of truth regarding their assets, creating an unprecedented level of transparency. Additionally, DeFi products can be constructed around this data, allowing users to hedge against the fractional reserve activities of traditional off-chain institutions.

## Proof of Reserve for Cross-Chain Assets and Wrapped Token Bridges

As a highly flexible and transparent oracle network model, Proof of Reserve helps accelerate the growth of DeFi by providing collateralization data on a wide array of assets and unlocking [cross-chain](https://chain.link/cross-chain) liquidity. As Chainlink is blockchain-agnostic, Chainlink PoR feeds can be constructed to provide collateralization data on any cross-chain asset settled on any smart contract-enabled blockchain.

### Proof of Reserve for Wrapped Token Bridges

Wrapped token bridges help create more capital efficiency in the DeFi ecosystem but introduce risks through the potential of undercollateralized wrapped assets. Chainlink PoR can be utilized to monitor the collateralization of wrapped assets in wrapped token bridges.

BGD Labs integrated Chainlink PoR into Aave on Avalanche to help ensure wrapped tokens in Aave markets on Avalanche are sufficiently collateralized. This solution involves a smart contract that acts as a registry for pairs of asset addresses and Proof of Reserve feed addresses. For each asset in the Avalanche deployment of Aave, the contract checks whether the Proof of Reserve feed value is equal to or greater than the total supply of the asset. If any asset on the list does not meet this requirement, a list of assets is outputted, and emergency actions may be performed. Depending on which version of the Aave protocol is being utilized, these can involve disabling the borrowing of all pool assets and freezing the assets in question or freezing the assets and setting their loan-to-value ratio to 0, removing the ability for these assets to be calculated as collateral on the platform.

Through trust-minimized mechanisms, the novel proof of reserves solution aims to validate that centralized wrapped assets or smart contracts such as cross-chain bridges can prove their reserves in real-time on-chain, enabling the Aave protocol to react and apply protections if an anomaly is detected.

[Swingby is using Chainlink PoR](https://chain.link/case-studies/swingby) to help secure its cross-chain bridge and protect users by preventing wrapped tokens from being minted or swapped if the reserves backing them become undercollateralized.

## Proof of Reserve for Liquid Staking Derivatives

Liquid staking derivatives are a tokenized representation of staked native assets. They are critical for unlocking more capital efficiency and supporting the growth of the DeFi ecosystem. Chainlink PoR feeds can be used to provide increased transparency for liquid staking derivative tokens, enabling anyone to verify whether liquid staking tokens are fully backed by staked native tokens.

## Proof of Reserve As a DeFi Circuit Breaker

An important tool for promoting stability and mitigating systemic risk in the DeFi ecosystem is a circuit breaker. Circuit breakers can help mitigate the extent of common hacks and exploits, prevent protocol insolvencies, decrease systemic risks, and more.

Aave is using Chainlink Proof of Reserve to validate that centralized wrapped assets or smart contracts such as cross-chain bridges can prove their reserves in real-time on-chain, enabling the protocol to react and apply protections if an anomaly is detected. If you’d like to learn more about this use case, read [DeFi Circuit Breakers With Chainlink Proof of Reserve and Automation](https://blog.chain.link/defi-circuit-breakers/).

## Conclusion

Chainlink Proof of Reserve provides both the growing DeFi ecosystem and the traditional financial system with a way to boost the transparency of their operations through definitive on-chain proof of any asset’s true collateralization. As the smart contract ecosystem grows, it is critical to ensure market failures caused by opaque operational processes and toxic collateral are consigned to history. With Chainlink Proof of Reserve, the DeFi ecosystem is well-positioned to scale and help secure the next generation of trust-minimized financial products.

If you want to know more about Chainlink Proof of Reserve, visit [the PoR product page](https://chain.link/proof-of-reserve). If you’re a developer and want to integrate Chainlink Proof of Reserve into your smart contract applications, check out the [developer documentation](https://docs.chain.link/) or [reach out to an expert](https://chain.link/contact?ref_id=education_hub).

**DeFi’s Permissionless Composability is Supercharging Innovation**

Last Updated Date:

August 14, 2024

DEFINITION

Permissionless composability in DeFi means developers can access key Web3 infrastructure without permission.

**Key Takeaways**

* DeFi composability allows developers to focus on their core business logic by leveraging permissionless and censorship-resistant infrastructure
* A multitude of DeFi applications (“Money LEGOs”) can be connected in tandem to create previously unimaginable use cases and financial products
* The traditional financial system has limitation on practical composability due to its permissioned nature, high barrier to entry, costs, and more
* Composability of DeFi applications requires due diligence on each protocol utilized to reduce systemic risk for the DeFi ecosystem as a whole

Since the launch of programmable [smart contracts](https://chain.link/education/smart-contracts), the blockchain ecosystem has blossomed into a borderless and permissionless landscape that supports a wide array of decentralized applications (dApps) running in parallel.

The first wave of applications were focused on using the blockchain to create digital tokens and track their ownership. However, the newest wave of dApps have evolved beyond ownership to unique methods of management and transfer that resemble and expand upon current traditional financial products. Collectively known as [Decentralized Finance (DeFi)](https://chain.link/education/defi), this parallel financial system is [worth over $100B](http://defipulse.com/) and is made up of decentralized exchanges, collateralized loans, lending and borrowing platforms, leveraged trading, synthetic assets, prediction markets, payment networks, and much more.

A key property accelerating the innovation and adoption of DeFi is the **permissionless composability** available to developers. Composability is a design principle that allows various different components within a system to be combined together to meet any specific use case requirements. DeFi is unique in that developers can leverage any combination of DeFi protocols together without requiring any special permissions, opening up a frictionless innovation cycle unlike anything we have seen in traditional finance.

In this article, we examine the limitations of the current financial system, how DeFi composability provides a permissionless financial architecture through the lens of a few in-production examples, and outline the systemic risks that such a system may introduce can be overcome.

**The Status Quo vs. DeFi**

The composability of financial applications is not a new concept. In fact, many of the popular user-facing applications used every day such as Uber, Lyft, and AirBnB are the result of financial composability. For example, Plaid and Stripe are financial services integrated throughout a multitude of web applications that provide native payment support to users. This greatly reduces their developer workload and speeds up the go-to-market strategy, since developers don’t have to build fiat payment infrastructure from scratch.

However, this form of financial composability comes with certain limitations.

**Permissioned Access**

Traditional centralized financial services are inherently permissioned to build upon, requiring “paper promises” based financial contracts between the two parties. This raises the barrier to entry and makes it very difficult for developers to create fully automated or impartial financial applications because there is the ongoing possibility that access is revoked at any time. The central entity now has control over key parts of the application, putting into question the deterministic guarantees the third-party developer seeks to provide.

DeFi turns this dynamic on its head by being inherently permissionless, creating an open foundation from which any developer can get immediate access to financial infrastructure that operates with high levels of tamper-resistance and reliability. This allows for truly impartial and deterministic applications that run as coded and are incapable of being shut down. Plugging into DeFi infrastructure requires no approval from the original developers, leading to seamless innovation without any central chokepoint.

**Reduced Transparency**

Traditional financial services are typically opaque or subject to information asymmetry, where the public is provided much less insight into the backend infrastructure. This creates unknown levels of risk exposure and reduces the ability to perform risk management. For example, financial composability enabled the creation of mortgage-backed securities via combining pre-existing consumer mortgages. Many deemed these financial products incredibly safe due to their diversification and AAA ratings given by traditional rating agencies. However, in 2008 it was revealed that many of these securities were backed by toxic subprime loans, triggering a global financial crisis. Had there been more transparency and visibility to a wider audience, such an implosion may have been prevented from occurring.

In contrast, DeFi products have transparency by default; as not only are they built upon open-source technology, but every transaction and interaction between users and dApps is recorded in an open, immutable ledger distributed around the world. While it might be months or years before a centralized cryptocurrency exchange is discovered to have gone insolvent, DeFi’s solvency and health is always subject to the collective observation and analysis of a large open-source community where anyone can point out fraud and systemic risk.

**DeFi Composability**

The modular composability of the DeFi ecosystem enables developers to focus on their core business logic, knowing they can always access key infrastructure without any permission required. With DeFi, when a developer creates a new token, they do not have to build their own exchange or pay to get it listed on some proprietary platform in order to support trading and the creation of liquidity. Instead, they can list their token on a pre-existing [decentralized exchange (DEX)](https://chain.link/education-hub/what-is-decentralized-exchange-dex) that has been thoroughly audited and contains an existing user base. This grants token holders immediate access to liquidity and different financial use cases with it, greatly expanding the utility of their token.

Some examples of the decentralized infrastructure in the background making DeFi applications possible include:

* Smart contract enabled blockchains ([Ethereum](http://ethereum.org/" \t "_blank))
* Tamper-resistant oracle networks ([Chainlink](https://chain.link/))
* Persistent data storage/web hosting ([IPFS](http://ipfs.io/))
* Censorship-resistant domain names ([ENS](http://ens.domains/))
* Reliable data queries and indexing ([The Graph](http://thegraph.com/))

Listing a token on a DEX is a quite simple example of composability, but this structure can be extended by connecting new DeFi applications to existing applications like ‘[Money LEGOs](https://medium.com/totle/building-with-money-legos-ab63a58ae764)’.

Some different money LEGOs in DeFi include:

* Order Book Exchanges ([Loopring](http://loopring.org/" \t "_blank), [dYdX](https://dydx.exchange/" \t "_blank))
* Automated Market Makers ([Bancor](http://bancor.network/" \t "_blank), [Sushi](http://sushi.com/))
* DeFi Aggregators ([1inch](http://1inch.exchange/), [Alpaca](https://www.alpacafinance.org/))
* Stablecoins ([Liquity](http://liquity.org/" \t "_blank), [Fei](https://fei.money/" \t "_blank))
* Money Markets ([Aave](http://aave.com/" \t "_blank), [Compound](http://compound.finance/))
* Synthetic Assets ([Synthetix](http://synthetix.io/" \t "_blank), [Alchemix](http://alchemix.fi/" \t "_blank))

These are just some of the many building blocks that can be connected in various combinations to create a structure that is greater than the sum of its parts. To note, many of the above listed applications actually fall under multiple categories meaning the same applications can connect in various ways to create differing combinations.

*“One of the biggest value propositions of DeFi is the interoperability by default. We have a financial system, which is accessible for the wider ecosystem. This means that anyone can build a product by combining two protocols, such as Aave and Synthetix, and provide a new user experience. If that product is good, it will get network effects quickly since liquidity moves in an interoperable fashion as well. That’s something that is far more powerful than we have in current financial systems.”  
–Stani Kulechov, Founder and CEO of Aave*

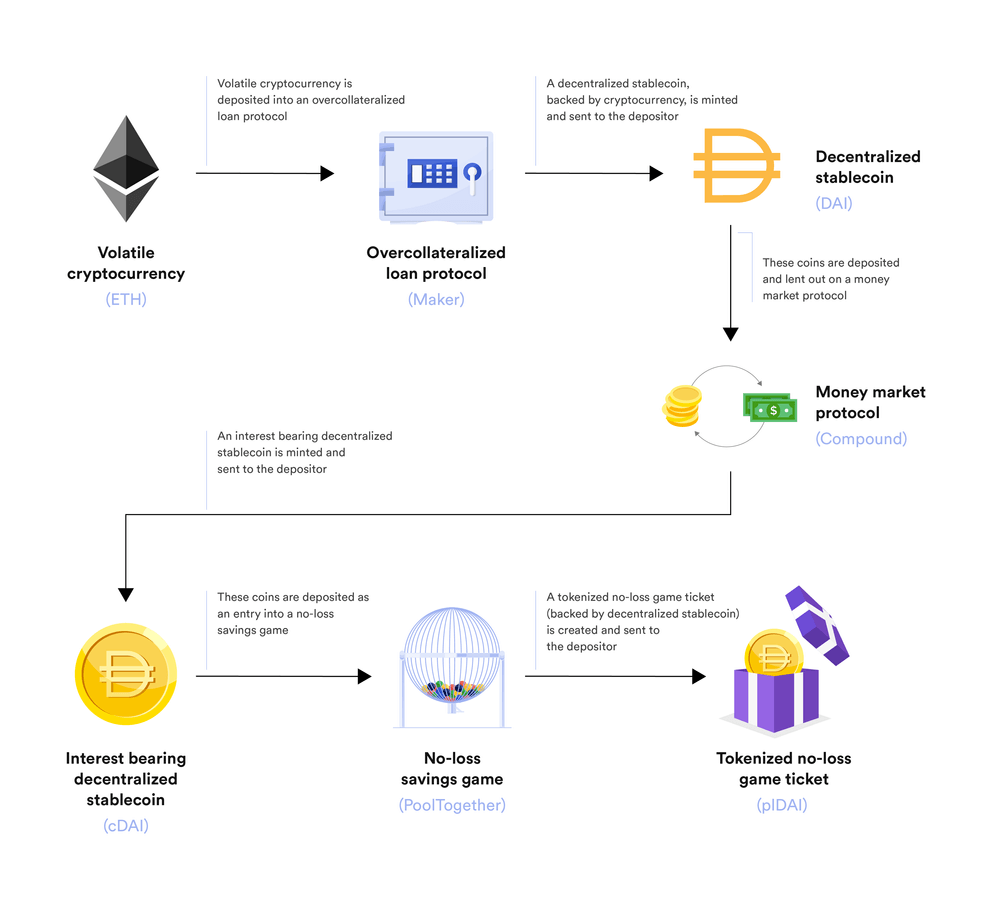
**Composability Squared**

A key property of DeFi composability is that it enables a chain of decentralized applications to be connected together in tandem. This increases capital efficiency as assets can be used within multiple applications at a time, with near zero friction costs and no permission required. It also fosters a growing network effect where every new DeFi application makes every other pre-existing DeFi application even more powerful and useful.

For example, while a user can gain working capital by minting decentralized [stablecoins](https://www.investopedia.com/terms/s/stablecoin.asp" \t "_blank) via opening an overcollateralized loan, these stablecoins become even more useful when deposited into a decentralized money market and [tokenized](https://blog.chain.link/tokenization/) to become non-custodial interest-bearing stablecoins. This means while the underlying stablecoins in the money market are being lent out to borrowers and actively earning interest, the newly created interest bearing tokens, which represent ownership of the stablecoin deposit, can be used within other DeFi applications or even used to pay for goods and services.

This composability can be further extended by multiple users pooling their interest-bearing stablecoins together to create a permissionless no-loss savings game —  a dApp where all the interest earned on the pooled stablecoins within a certain time period is awarded to one lucky winner, where afterwards everyone can withdraw the value of their original deposit. This no-loss savings game can tokenize user deposits into tradable tickets (a claim on the deposit) and continue the cycle of DeFi composability.

The entire process above already exists within DeFi, involving a combination of Ethereum, Chainlink, MakerDAO, Compound, and PoolTogether. By leveraging Maker’s DAI stablecoin, Compound’s money market cTokens, and [Chainlink VRF](https://chain.link/vrf), PoolTogether was able to create an innovative decentralized application without having to build a stablecoin, bootstrap a money market protocol, or figure out how to get a verifiable on-chain source of randomness.



A set of Money Legos showcasing DeFi’s permissionless composability

**DEX Aggregation**

A DeFi application that also makes heavy use of composability is [1inch.exchange](http://1inch.exchange/). This is a decentralized exchange (DEX) aggregator that fetches liquidity from across all DEXs on Ethereum, allowing users to swap tokens on-chain at the lowest slippage possible. 1inch splits large trades into multiple orders that can then be settled across multiple DEXs within a single transaction to achieve the most optimal exchange rate.

1inch creates a superior experience for users; instead of needing to check and compare many different DEXs for their current exchange rates, users can only have to navigate to a single application and immediately get access to all the liquidity residing on Ethereum.

**Flash Loans**

Another application harnessing composability is decentralized money market [Aave](http://aave.com/" \t "_blank), which increases the capital efficiency and yield of deposits by enabling [superfluidity](https://tokeneconomy.co/superfluid-collateral-in-open-finance-8c3db15efac" \t "_blank) of assets through flash loans. These are temporary uncollateralized loans that must be paid back (plus a small fee) within the same transaction. If a flash loan borrower is unable or does not pay back their loan immediately, then the transaction as a whole reverts, protecting the protocol and its lenders from any defaults.

Flash loans are a powerful concept; not only are they atomic (either succeeds or reverts, no in-between), but they allow anyone to temporarily access a large amount of capital to take advantage of an inefficiency or leverage up an opportunity, ultimately leveling out the playing field for DeFi. [Flash loans](https://chain.link/education-hub/flash-loans) can be used to perform profitable arbitrage between DEXs, seamlessly leverage up a loan, switch out the collateral and/or debt in a loan, and numerous other use cases all within a single transaction.

**Money LEGOs as Collateral**

In addition to the above, Aave has also rolled out support for [unique collateral types](https://medium.com/aave/the-uniswap-market-is-live-on-aave-protocol-12b5a4cc5e2) that take advantage of tokens generated from other DeFi applications. For example, the first new unique collateral type is liquidity pool shares from Uniswap, an Automated Market Maker ([AMM](https://chain.link/education-hub/what-is-an-automated-market-maker-amm)) DEX. Aave was able to roll this feature out in a manner of only a few weeks, due to the fact they utilized Chainlink oracles which already supported the price feeds required. By connecting to [Chainlink Price Feeds](https://chain.link/data-feeds), Aave was able to seamlessly implement advanced forms of composability in a secure manner.

For context, when a user deposits funds into a liquidity pool on Uniswap (where each pool requires two tokens), they receive back UNI pool tokens which represent a claim on their funds. These UNI pool tokens can then be transferred and deposited into the Aave money market and used as collateral within a loan. This enables a high degree of capital efficiency for market makers as they are now able to provide liquidity and earn trading fees on Uniswap, while at the same time borrow against that capital. They can then even use those borrowed funds to deposit even more liquidity onto Uniswap, creating leveraged long exposure to Uniswap trading fees and the assets within the pool.

**Potential Risks of Composability**

Even with all the benefits, developers should be careful to not build on a foundation of quicksand when utilizing the property of composability. The risks involved with the development of DeFi composability can be refined down to four core properties. The first is the inherent protocol level risk of the blockchain network that decentralized applications operate upon. If this baselayer is unable to come to consensus or gets tampered with by malicious attackers, then everything that runs on top is vulnerable to manipulation as well. This is not entirely unique to DeFi composability, but is something always in consideration regarding decentralized application risk.

The second is the unique implementation risks of each smart contract application individually on its own. Every application is based on its own design trade-offs in order to meet specific needs for each desired use case. For example, there is the potential for software bugs in an applications source code that could cause a decentralized application to behave in an unexpected manner. To mitigate these vulnerabilities, the Chainlink protocol has undergone multiple smart contracts security audits, including audits on each new product feature, as well as offering generous [bug bounties](https://hackerone.com/chainlink) and having fully [open-source](https://github.com/smartcontractkit/chainlink) code. All of these risk mitigation tactics are in addition to the defense in depth approach taken through employing decentralization at the data source, node, and network levels. This ensures users have full confidence before they even begin to integrate oracles into their application.

The third risk involves the expansion of the attack surface of all of the above when composing multiple smart contracts together. While two particular decentralized applications may be secure in isolation, the combination of the two may not. An increase in an application’s composability increases the attack surface in such a way that is greater than the sum of its parts. This creates more edge cases that need to be preeminently mitigated against to ensure a smooth operation. This composability risk can also take the form of utilizing potentially subpar collateral within another Defi application such as a money market, for which is only as strong as its weakest collateral token supported.

Lastly the fourth risk involves user knowledge and accessibility. A user who doesn’t understand the application they are utilizing is more likely to take on more risk than they realize. It is for this reason user education and transparency about risk is so important to ensuring a healthy ecosystem. DeFi composability can quickly get highly complex so it is key that each step in the process is broken down to a level that users can understand what they are putting their money into.

For all of the risks above, it is critical that those in the open-source community actively participate in the analysis of DeFi applications and the composability being used in order to preemptively mitigate any issues before they arise. Composability enabled applications have lots of moving pieces that each needed to be ensured to be of the highest quality. In addition, it is key to set and implement industry-wide standards to ensure best practices across the ecosystem and bolster this security through bug bounties, audits, hackathons, and other forms of developer engagement. By doing so, a stronger and more resilient financial ecosystem is created and user funds are safeguarded in the best manner possible.

**Conclusion**

In summary, DeFi has been built as a new financial ecosystem that operates alongside the current traditional financial system, yet offers unique advantages of permissionless composability, censorship-resistant access, and full transparency. In particular, DeFi composability opens up the ability for any developer to launch new innovative financial applications at an accelerated rate because they don’t rebuild core infrastructure or have to rely on the centralized and permissioned financial services of today.

The open-source, permissionless nature of DeFi facilitates a level playing field, which fosters an environment that requires constant innovation to retain market share. The DeFi applications that make use of composability today are setting the foundation for the next generation of dApps that will utilize even more advanced forms of composability. There are limitless use cases to discover and applications to be built. The future of a permissionless modular financial future looks bright indeed.