BINANCE RESEARCH

Oracle-Less: Challenging the Status Quo

September 2023

Jie Xuan Chua, CFA
Brian Chen

Table of Contents

1 Key Takeaways

- Oracles connect the on- and off-chain worlds, providing blockchains with access to real-world data. However, past cases of exploits due to oracle manipulations remind us that the usage of oracles can introduce trust and reliability concerns.
- By eliminating dependency on oracles, oracle-less protocols can help projects combat price manipulation, increase self-reliance, and save on oracle-related costs.
- To understand how oracle-less protocols work, we examined several projects across the lending, derivatives, and non-fungible tokens space. We have observed creative workarounds to facilitate pricing, liquidation, and other mechanisms, without relying on oracles.
- While oracle-less protocols offer an alternative to the existing landscape dominated by oracles, there are trade-offs relating to complexity, efficiency, and design constraints that need to be considered.
- Looking ahead, we believe that there exists sufficient room for both oracle-less and oracle-dependent protocols to thrive. Given the trade-offs associated with each solution, developers and users may find different use cases in which one solution is more appropriate than the other.

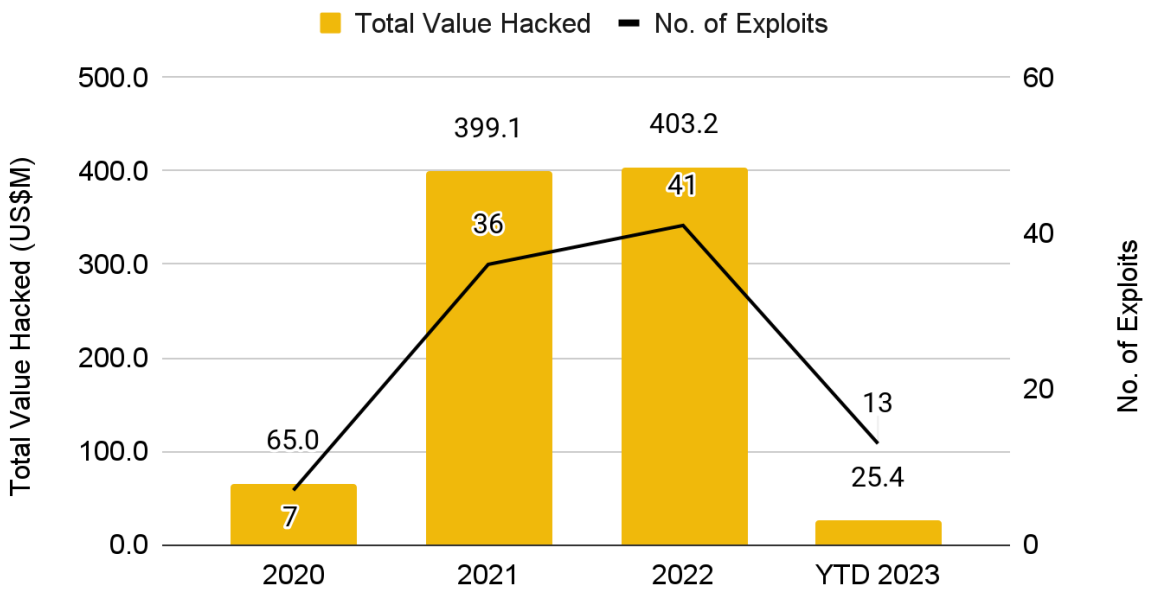
2 The Oracle Problem

Oracles connect the on- and off-chain worlds, providing blockchains with access to real-world data. From prices of crypto assets to results of a football match, oracles can fetch various kinds of external data, which can be further integrated into the crypto ecosystem. Oracles effectively expand the capabilities of blockchain networks by allowing tasks to be executed based on real-world inputs.

However, the usage of oracles introduces trust and reliability concerns. Since real-world data points tend to be non-deterministic (e.g. different bitcoin prices across exchanges), the reliability of outputs by oracles requires trust, thereby disrupting trustless execution typically associated with smart contracts.

Additionally, oracles represent potential points of failure that may be vulnerable to manipulation. There have been numerous instances of price oracle manipulation in the past, resulting in millions of dollars lost to exploits.

Figure 1: Over US$892M has been lost due to oracle-related exploits since 2020



Source: Chainalysis, DeFi Llama, De.Fi, Binance Research, data as of Sep 18, 2023

An estimated US$892M has been exploited due to oracle-related manipulations over the past 3+ years. In many instances, actors drive up the prices of low-liquidity tokens on targeted protocols before swapping their artificially inflated tokens to other tokens, or using them as collateral to take up loans in lending markets. On the bright side, the amount lost due to oracle-related exploits has decreased significantly in 2023, likely caused by a combination of increased focus on security and a broad decline in DeFi TVL.

3 Let's Go Oracle-Less

Recent research has addressed the aforementioned concerns related to oracles, and we have witnessed much progress on this front. Work has been done by teams behind oracles in multiple areas which include, but are not limited to, decentralization, transparency, and data verifiability.

As a thought experiment, let's take it a step back and imagine a world where the reliance on oracles has been eliminated altogether. In such a world, how would blockchain projects forgo using external data? That's where oracle-less protocols come into play.

As the name suggests, **oracle-less protocols are not dependent on oracles to function**. Instead, alternative mechanisms are used to achieve the same results. As a result, oracle-less protocols offer several advantages:

- **Eliminating oracle-related price manipulation:** Given that oracle-less protocols are not reliant on external price feeds, oracle price manipulation by rogue actors is impossible.
- **Enhanced security and self-reliance**: Integrating with third-party oracles increases risks for a protocol by expanding the potential attack surface. Being self-reliant reduces the risk of attacks related to oracle vulnerabilities.
- **Lower cost:** Without engaging the services of oracles, protocols save on fees that would have otherwise been paid to them.

Let's explore a few case studies and observe how oracle-less protocols work.

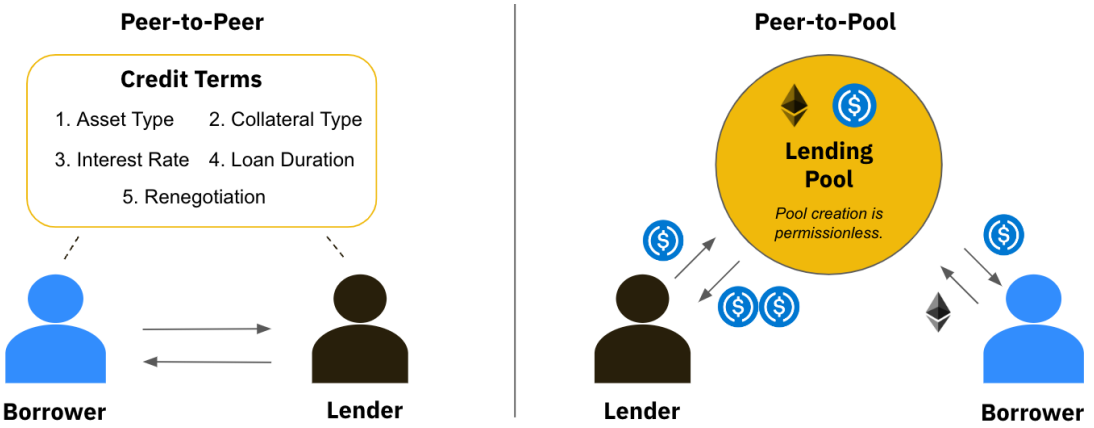
3.1 Lending

Conventional lending protocols typically rely on oracles for price information to facilitate the liquidation process. However, this dependency introduces a potential attack vector – namely, oracle price manipulation. Malicious actors can exploit this weakness to skew price feeds and swiftly drain a platform's funds. Prominent instances of such exploits include last year's Mango Markets breach and the more recent attack on EraLend in July this year. To address these vulnerabilities, several protocols have pioneered oracle-free solutions that remove the need of external price feeds.

Prevailing oracle-less solutions in DeFi lending fall into two main categories: peer-to-pool and peer-to-peer models. The peer-to-pool model excludes price oracles by enabling permissionless pool creation, thereby shifting the responsibility of asset pricing onto the users themselves. Given that pool parameters are sensitive to market dynamics, this approach requires active position management. On the other hand, the peer-to-peer

model serves as a straightforward method for lending and borrowing, allowing both parties to directly interact and establish terms of credit.

Figure 2: Illustration of peer-to-peer and peer-to-pool models



Source: Binance Research

To illustrate how each of these models functions in practice, we examined two case studies below. Note that the mention of specific projects does not constitute an endorsement or recommendation by Binance. Instead, the projects cited are merely used for the purposes of illustrating the aforementioned concepts. Additional due diligence should be taken to better understand the projects and associated risks.

Ajna Finance

Launched in July 2023, Ajna is a peer-to-pool lending and borrowing platform that operates without requiring governance or external price feeds. The protocol seeks to solve two persistent challenges in the DeFi space: limited capital efficiency for long-tail assets and dependency on price oracles. Ajna addresses these issues by requiring users to actively monitor their positions and by enabling the creation of permissionless pools with flexible parameters.

Mechanics

Ajna Finance employs three features to eliminate oracle dependencies:

- **Permissionless pool creation**
- **Lending with liquidity ranges**
- **Liquidation bond**

On Ajna, users can create permissionless pools that aggregate the lending and borrowing activities for specific quote tokens, backed by specific collateral tokens. Pool creators can independently set the initial interest rates for each specific token pair. Rates are adjusted based on utilization and change every 12 hours in 10% increments.

Compared to other protocols, lending on Ajna requires a greater extent of active management. Lenders must select a price, or a “price bucket,” at which to lend their assets.

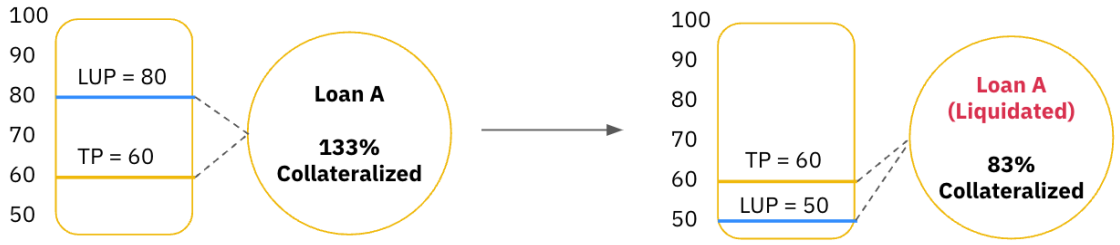
These price buckets correspond to four types of liquidity, each with varying degrees of risk and reward. The categorization of liquidity is determined by its state – whether it is active, ready to be used, or unutilized. These inform parameters such as:

- **Threshold Price ("TP"):** set by the borrower and is a loan's debt divided by the collateral.
- **Neutral Price ("NP"):** set at origination, is usually some number above the TP, and acts as the liquidation price of the loan.
- **Lowest Utilized Price ("LUP"):** moves freely and is defined as the lowest collateral price bucket against which someone is actively borrowing.

These parameters have an impact on the interest earned and dictate whether a position is over-collateralized or under-collateralized. As these parameters are dynamic and change in response to the borrowing and lending activities within the pool, positions are required to be managed actively.

A position is eligible for liquidation when the loan's TP crosses above the pool's LUP. Anyone can trigger a liquidation by posting a liquidation bond for the loan. (A liquidation bond is effectively a bet on the outcome of a collateral sale.) In effect, **by having users step in to trigger the liquidation process, the protocol does not need to rely on oracles** as typically seen in conventional lending protocols.

Figure 3: Illustration of an overcollateralized loan becoming undercollateralized



Source: Ajna Finance Whitepaper, Binance Research

In essence, Ajna eliminates the need for external price feeds by allowing users to serve as their own price feeds. Both lenders and borrowers must actively manage their positions in line with the market price to avoid liquidation or the loss of interest.

Note that Ajna has only been live for around two months at the time of writing, and users should do their own due diligence before interacting with the protocol. For example, the protocol has recently discovered a grief vector that could impact borrowers.

PWN Finance

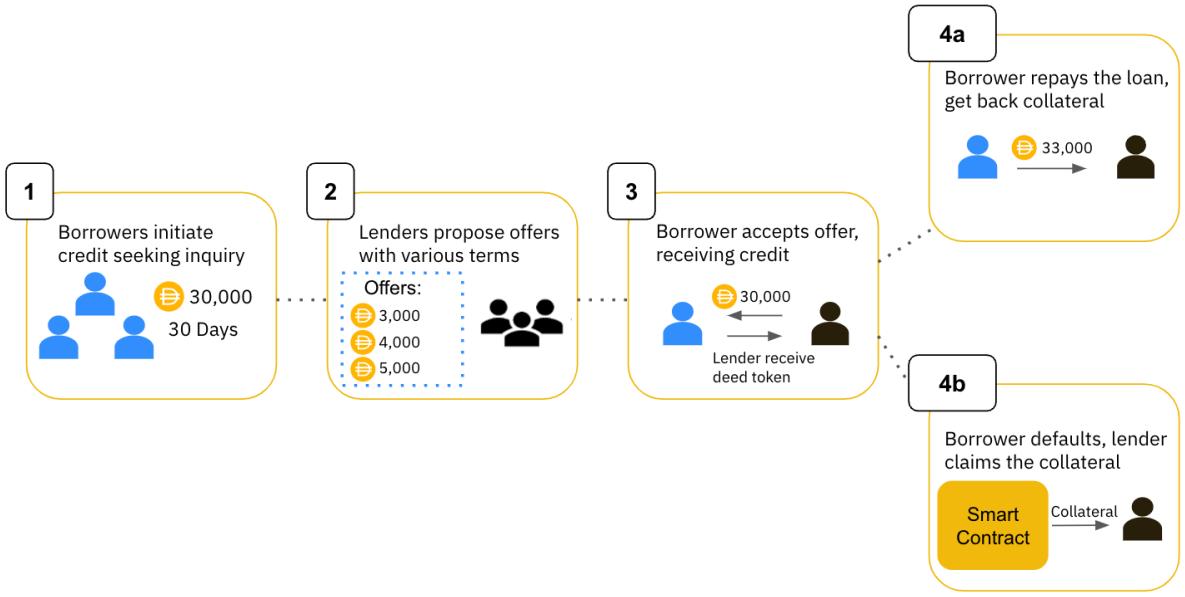
PWN Finance is a peer-to-peer lending protocol designed to support an array of fungible and non-fungible assets without requiring price oracles or lending pools. The platform facilitates direct matches between borrowers and lenders, empowering them to set their own credit terms. These terms can range from short to long durations and can accommodate various token standards, such as ERC-20, ERC-721, and ERC-1155.

Mechanics

The PWN loan process involves four key steps:

1. Borrowers begin the process by listing their collateral and credit-seeking inquiries (e.g., type of asset, loan amount, loan term).
2. Lenders submit their credit terms to borrowers for consideration.
3. Once terms are agreed upon, borrowers receive the loan amount while lenders receive a deed token which represents the lender's claiming rights. Deed tokens are transferable, granting lenders the flexibility to exit their positions whenever they like.
4. Upon maturity, borrowers can either repay the loan with interest or, in the case of a default, lenders can claim the pledged collateral.

Figure 4: PWN Finance loan process



Source: PWN Finance, Binance Research

PWN Finance's peer-to-peer model operates on the most direct form of lending and **eliminates the use of oracles by having borrowers and lenders agree upon a set of credit terms right at the onset.** Given that the loan duration is fixed, a lender can only claim the collateral if the borrower fails to repay the loan at the end of the term. In this way, even if the value of collateral fluctuates during the loan period, there is no impact to the borrower as it would not trigger liquidation. It is also due to this mechanism that PWN is able to operate without relying on an oracle.

That said, **it is key to note that lenders undertake a risk that collateral values may fall below the value of loans at the end of the term.** In this case, borrowers may be incentivized to not repay the loan, and to forfeit their collateral instead. Lenders may end up being made worse off in such a situation.

3.2 Derivatives

Derivatives are financial instruments that derive their value from underlying assets. In the DeFi derivatives sector, price oracles are extensively used to facilitate liquidation and determine the outcomes for derivatives contracts.

More recently, we have witnessed the emergence of oracle-less derivatives protocols. Currently, these solutions mainly employ Uniswap V3-like Automated Market Makers ("AMMs") as their foundational layer.

In leverage trading platforms, traders' positions are based on Liquidity Provider ("LP") tokens. **Because the value of the underlying asset is implicitly encoded within these LP tokens – along with other variables like liquidity range – there is no need for price oracles for asset pricing**.

In the case of options protocols, since a Uniswap V3 LP position essentially serves as a short put-selling position, **developers leverage this feature to redefine options pricing mechanisms without relying on the Black-Scholes-Merton ("BSM") model**, thereby avoiding the use of oracles.

In the following section, we discuss two prime examples to further elaborate on their underlying concepts.

InfinityPools

InfinityPools is a leverage swap platform that aims to offer unlimited leverage on any asset pair without liquidation risk or the need for oracles, ambitiously aiming to become a new DeFi primitive. The platform employs Concentrated Liquidity Market Makers ("CLMMs") as its foundational layer, thereby enabling leverage positions that are secured by LP tokens. This ensures that sufficient liquidity is available for unwinding leverage positions, while the **pricing of those trades is predetermined through the mathematical structure of the LP tokens themselves**.

Note that the protocol is still under development and is in public beta. Information has been sourced from publicly available sources and interested readers are encouraged to do their own research.

Mechanics

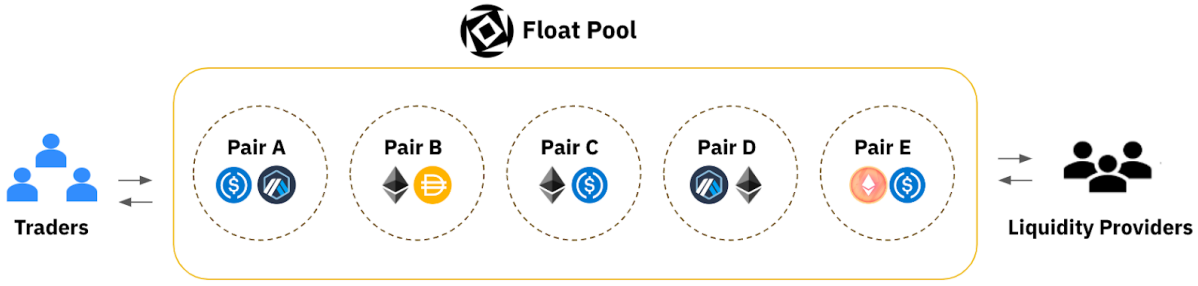
Two core components enable InfinityPools' oracle-free operation:

- **Float pool**
- **LP token-based positions**

Leverage trading on InfinityPools occurs within a protocol-owned liquidity pool known as the Float Pool. This pool is a Uniswap V3-like concentrated liquidity pool, drawing its liquidity from providers who contribute either UNI V3 LP tokens or raw liquidity. These assets are then lent to traders who opt to open leveraged positions. The borrowed LP tokens serve as the backbone of traders' positions. Traders are obligated to repay either one of a mix of the underlying assets of the LP tokens, with the repayment value equating to the original borrowed amount. The collateral requirements for traders are dictated by the liquidity range associated with each LP token. **This structure not only obviates the need of external price feeds but also guarantees ample liquidity** to secure each leveraged position.

For example, assume a scenario in which a trader borrowed an ETH/USDC LP token valued at US$2,000 and deployed it in a liquidity range centered at US$1,800. Regardless of whether the price of ETH rises or falls, the trader must return assets that are worth US$2,000. To ensure repayment of this amount if the price of ETH declines – whether it stays above or dips below US$1,800 – a collateral of 200 USDC or 0.11 ETH is required. The entire structure operates self-sufficiently within the protocol's liquidity pool and is defined by the CLMM LP mechanism.

Figure 5: Simplified illustration of InfinityPools structure



Source: InfinityPools, Binance Research

InfinityPools offers an innovative approach to leverage trading by capitalizing on the unique features of CLMM LP tokens. In theory, positions are liquidation-free and can open on any asset with extremely high leverage. However, leverage is still somewhat limited by the liquidity range, and tradable assets are subjected to the availability of liquid assets.

Panoptic

Panoptic is an oracle-free perpetual options protocol that offers a distinctive way for trading on-chain options. Recognizing the resemblance between the payoff of an Uniswap V3 LP and a put-selling position, the Panoptic team devised a new method for pricing and trading options on-chain that does not require the BSM model. Given that the BSM model requires input on variables such as the underlying asset price and volatility for options pricing, **doing away with the BSM model means that the protocol is not reliant on oracles to provide these inputs.**

Note that the protocol is currently in a gated beta testing phase, and readers are encouraged to do their own research.

Mechanics

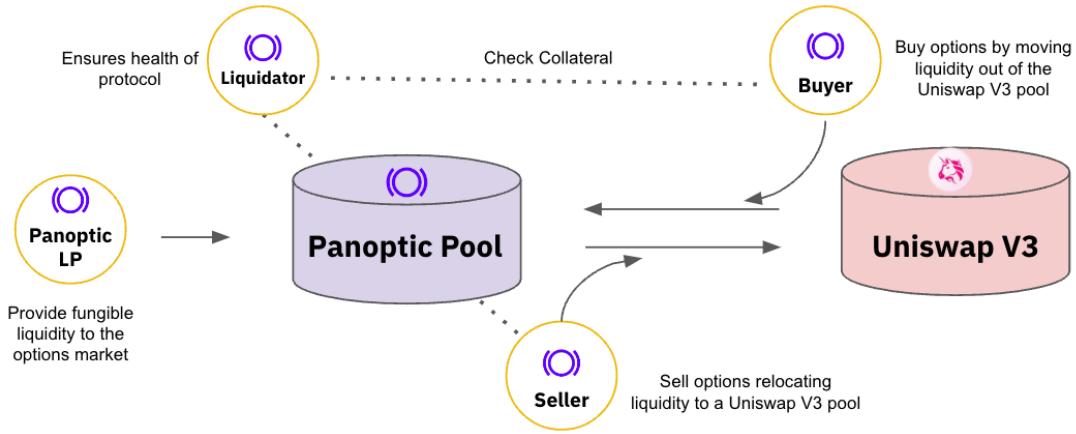
Panoptic achieves its oracle-free quality through an unique options pricing method called Streamia, a term representing the continuous flow of options premiums. In traditional options pricing, the BSM model is heavily used, which necessitates the use of an oracle for real-time data retrieval.

Streamia eliminates the need for an oracle by basing fees on whether an option is within a specified range. Unlike traditional models where buyers pay a one-time upfront option premium, the pricing of an option in Panoptic is path-dependent and will increase at each block if the spot price is within range of the option's strike price.

Assume a scenario in which an options seller initiates a position on the USDC/ETH pair with a strike price of US$2,000 and the market price of ETH at US$1,800. Assuming a 10% width, the bounds are set at US$2,200 and US$1,818 (US$2,000/1.1). Stremia fees will accumulate when the price is within range (between US$2,200 and US$1,818) and will not increase when it is out of range.

As a quick overview of how the option mechanics work, selling an option on Panoptic requires sellers to post collateral, either borrowed from liquidity providers or self-supplied. This collateral is then deployed to Uniswap V3. Option buyers, on the other hand, use Panoptic to borrow and shift the seller's LP tokens back into the Panoptic pool. As such, options trading on Panoptic involves moving funds between Uniswap V3 and Panoptic pool. By leveraging the option-like payoff structure of LP positions and the fluid movement of liquidity, Panoptic enables a new form of options trading.

Figure 6: Panoptic liquidity movements dynamic



Source: Panoptic, Binance Research

Panoptic's approach appears to offer a more dynamic way for trading crypto options. Its range-based premium calculation eliminates upfront payments, and the absence of the BSM model eliminates the need to rely on oracles for option pricing.

3.3 Non-Fungible Tokens (“NFTs”)

Traditional DeFi lending often hinges on the use of price oracles, a practice that extends to NFT-backed lending protocols as well. These protocols not only risk having a single point of failure due to their reliance on oracles but also grapple with challenges around asset valuation. **Accurately determining the floor prices of NFTs on-chain is a complex task, let alone objectively pricing individual NFTs with different rarity traits.**

The rise in the number of oracle-less NFT lending protocols is a positive development, providing an alternative to existing solutions. **Oracle-less NFT lending protocols predominantly adopt a peer-to-peer model.** They operate by directly connecting borrowers and lenders, enabling desired credit terms to be established. Freed from third-party involvement and the need of external price feeds, both parties rely on their own assessments of the value and potential of collateral when facilitating loans. Below, we explore two examples to understand their underlying mechanics.

Blend

Launched in May 2023, Blend is a peer-to-peer perpetual lending platform co-developed by the Blur team and Paradigm. By adopting a peer-to-peer model and a novel liquidation mechanism, Blend obviates the need for oracles, enabling both lenders and borrowers to autonomously determine credit terms that align with their financial objectives. Critical variables such as interest rate, LTV ratio, and loan duration are driven by market dynamics, affording greater flexibility to both parties.

Mechanics

A loan on Blend unfolds as follows:

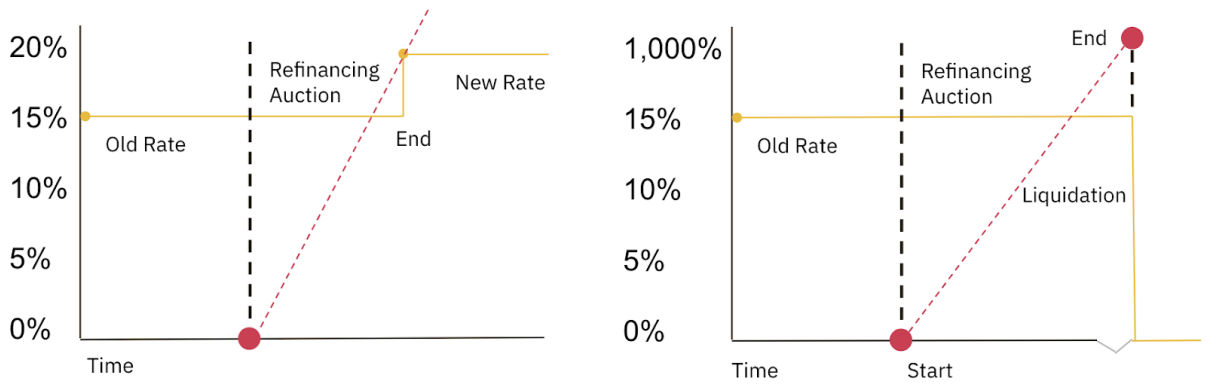
1. Lenders identify the specific NFT collection they are willing to accept as collateral for lending ETH.
2. Once a borrower accepts the offer, the NFT serving as collateral is locked into the smart contract.
3. The loan operates on a continuous basis and can be terminated either by the lender or the borrower.

Initially, lenders select the NFT collection they are comfortable with using as collateral. They must then specify the maximum amount they’re willing to lend, as well as the interest rate for the loan. When a borrower agrees to these terms, the collateral NFT is locked, and the lender starts accruing interest.

Both parties have the option to close the loan: the borrower can do so by repaying the principal plus interest, while the lender can initiate loan refinancing. This refinance functions as a Dutch auction in the interest rate space. Rates start as 0% and continue to

rise until another lender steps in or the rate hits a predetermined cap. At this point, the loan is considered insolvent and is subject to liquidation, allowing the lender to claim the collateral.

Figure 7: The Dutch auction scenarios



Source: Paradigm, Binance Research

By introducing a novel exit/liquidation mechanism in the form of a Dutch auction, Blend has no oracle dependencies. **Instead of relying on an oracle to determine when a position should be liquidated, lenders have the discretion to trigger a liquidation if they so wish.** Nonetheless, this also means that lenders should actively monitor their own positions and proactively step in should the risk-reward ratio no longer make sense.

NFTfi

NFTfi is another peer-to-peer lending protocol specializing in fixed-term NFT-backed loans. Much like Blend, NFTfi eliminates the necessity for oracles by functioning as a peer-to-peer matching platform. This allows borrowers and lenders to negotiate their own credit terms directly. As NFTfi provides fixed-term loans and Blend offers perpetual loans, they each create distinct risk-reward profiles for their users.

Mechanics

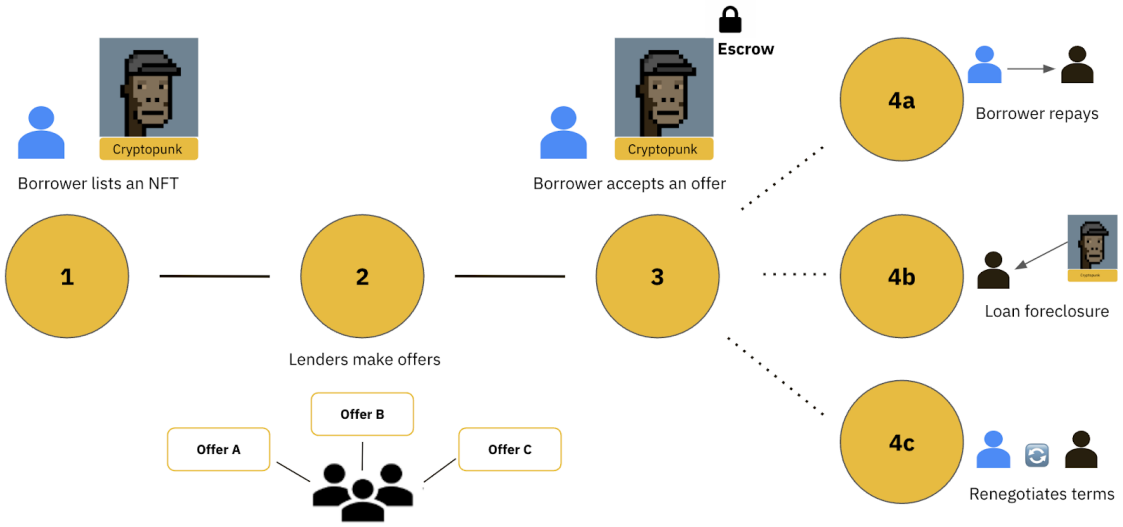
A loan on NFTfi is implemented as follows:

1. Borrowers list their NFTs, with an option to specify their desired loan terms.
2. Lenders, in search of opportunities, submit competing offers for an NFT.
3. A loan is formalized when the borrower accepts one of the offers.
4. At the loan's expiration, options include an extension or foreclosure by the lender if the borrower fails to repay.

The process begins with borrowers listing their NFTs and signaling their preferred terms. Lenders eyeing interest-earning opportunities propose their terms, keeping in mind that they might need to compete with other lenders who are interested in the same NFT. Upon loan initiation, the borrower receives the loan amount, and the NFT is escrowed in a smart contract. Loans can conclude in two ways: either the borrower repays the debt, or the

lender forecloses on the loan if the borrower defaults. Notably, NFTfi allows for loan renegotiations before or upon maturity, giving both parties the option to modify terms if repayment is not made on time.

Figure 8: How NFTfi works



Source: NFTfi, Binance Research

NFTfi operates effectively without the use of an oracle by utilizing a peer-to-peer model. Borrowers and lenders negotiate terms based on the market value and potential of the specific NFT collection. The option for renegotiation adds an extra layer of flexibility, enabling users to adapt to changing circumstances.

4 A Perfect Solution? Nothing Is.

While the lack of dependency on oracles insulates oracle-less protocols from risks associated with them, oracle-less protocols are not foolproof. As with any solution, there are trade-offs that should be considered by developers and users alike.

- **Greater complexity:** Workarounds to reduce reliance on oracles make oracle-less protocols generally more complex. In many cases, users take on additional burden, which may include more active position monitoring (e.g., manually tracking asset prices), having to do more intricate risk-reward analysis (e.g., determining acceptable loan terms in the case of lending), and perhaps, even potentially absorbing losses (e.g., when collateral value falls below that of the loan).
- **Oracle-less in theory but not necessarily in practice:** While the protocol itself may not be dependent on oracles, the reality is that users may still end up having to rely on external sources of data to make decisions. In some cases, the information source may turn out to be reliant on an oracle or a centralized data provider.
- **Reduced efficiency:** Liquidation in oracle-less protocols is less straightforward than oracle-dependent protocols. Instead of an automatic liquidation being triggered when price falls below a certain threshold, oracle-less protocols may involve manual user intervention, resulting in time lags and reduced efficiency.
- **Greater design constraints:** Without the ability to easily utilize external data via oracles, protocols may be limited in their design. For example, certain protocols do not support liquidations.

Ultimately, eliminating oracle dependency is not a straightforward or simple task given that alternative mechanisms need to be put in place to achieve the same result. Such **workarounds could introduce additional layers of complexity which would prove to be a challenge for mass adoption.**

Eliminating reliance on oracles is only the first step. The next would be to figure out how to keep things simple enough such that oracle-less protocols remain reliable and user-friendly.

5 Outlook and Closing Thoughts

Oracles are integral to the crypto ecosystem, serving as the bridge between on- and off-chain worlds by supplying real-time data and enabling the seamless operations of many DeFi protocols. However, the use of oracles can be a double-edged sword, creating vulnerabilities that malicious actors could potentially exploit.

Oracle-less solutions seem to offer a set of enticing alternatives that alleviate the risks associated with oracle. Nonetheless, the adoption of these alternative solutions is influenced by a myriad of factors and considerations, and it may be more appropriate in some cases than in others. For instance, due to differences in NFT rarity levels and traits, oracle-less solutions like a peer-to-peer model could be more suitable in NFT lending, as evidenced by the dominant borrowing volumes peer-to-peer NFT protocols boast. In DeFi, the majority of protocols continue to rely on oracles. Considering this, it is positive that oracles have made significant strides and advancements in recent years to enhance security and increase decentralization.

Looking ahead, **the landscape is not strictly a competition between oracle-dependent and oracle-less protocols.** Both have their own advantages and drawbacks, and may be more suitable in certain cases than others. While oracle-less protocols may attract specific user groups owing to their unique underlying mechanics, **it is unlikely that the majority of users will choose a protocol over another based on a single criterion of whether there is an oracle dependency.** Instead, project teams will need to evaluate what mechanisms and structures make more sense for what they have set out to achieve.

References

1. https://www.ajna.finance/pdf/Ajna_Protocol_Whitepaper_07-11-2023.pdf
2. https://pwn.xyz/PWN-Whitepaper.pdf
3. https://docs.infinitypools.finance
4. https://infpools.medium.com/introducing-infinitypools-or-how-i-learned-to-stop-worrying-and-love-leverage-9b44fc8367b6
5. https://panoptic.xyz/blog/black-scholes-streamia-defi-options-pricing-models
6. https://panoptic.xyz/blog/streamia-defi-native-options-pricing
7. https://panoptic.xyz/docs/intro
8. https://panoptic.xyz/research/defi-put-options-uniswap-backtest
9. https://www.paradigm.xyz/2023/05/blend
10. https://docs.nftfi.com/overview/introduction

New Binance Research Reports

The OP Stack: What's New?

A look at the growing OP Stack ecosystem

Navigating Crypto: Industry Map

An overview of different verticals in cryptostraction

Monthly Market Insights: September 2023

A summary of the most important market developments, interesting charts and upcoming events

Ethereum: Beyond The Merge

A deep dive into Ethereum's roadmap

About Binance Research

Binance Research is the research arm of Binance, the world's leading cryptocurrency exchange. The team is committed to delivering objective, independent, and comprehensive analysis and aims to be the thought leader in the crypto space. Our analysts publish insightful thought pieces regularly on topics related but not limited to the crypto ecosystem, blockchain technologies, and the latest market themes.

Jie Xuan Chua, CFA

Macro Researcher

Jie Xuan ("JX") is currently working for Binance as a Macro Researcher. Prior to joining Binance, he worked as a Global Investment Specialist with J.P. Morgan and had prior Equity Research experience at various fund houses. JX is a CFA charterholder. He has been involved in the cryptocurrency space since 2017.

Brian Chen

Macro Research Intern

Brian is currently working for Binance as a Macro Research intern. Prior to joining Binance, he worked as a DeFi researcher at a financial service startup and a Web3 education organization. He holds a Master of Finance degree from the University of California, Irvine ("UCI"), and has been involved in the cryptocurrency space since 2021.

Resources

Read more here

Share your feedback here