Bringing traditional capital efficiency to Solana.

Zodial

Zodial is the first DeFi lending protocol that can support arbitrary portfolio compositions through a unified approach, giving users full freedom to build their portfolios according to their convictions. Compared to traditional isolated market protocols, users can freely lend and borrow against their entire asset portfolio. This unlocks maximal capital efficiency and sophisticated trading and diversification strategies previously impossible in DeFi. Institutions can profit from the significant improvements to capital efficiency to better support large positions. To make this possible, Zodial uses an industry-first proof verification system which is essential to achieve maximum capital and collateral efficiency for any portfolio.

Supported by Solana Superteam Germany

Audit in progress

DeFi Lending Infrastructure is Broken

DeFi lending only captures around 2% of the ~$3 trillion crypto market ($60B). Current protocols generate ~$160M in profit from ~2.5% commission, indicating significant room for growth. This massive gap exists in large parts due to fundamental design and UX limitations in current protocols.

Isolated Markets Create Fragmented Capital

Capital is siloed in each market, requiring users to overcollateralize and lock up significantly more capital than theoretically necessary. Diversification is severely restricted and requires constant manual rebalancing of collateral. Single-asset exposure leads to early liquidations.

Strategies are Limited

Basic hedging strategies are impossible to implement, multiple platforms need to be used for cross-market risk management and no unified view of portfolio risk is available.

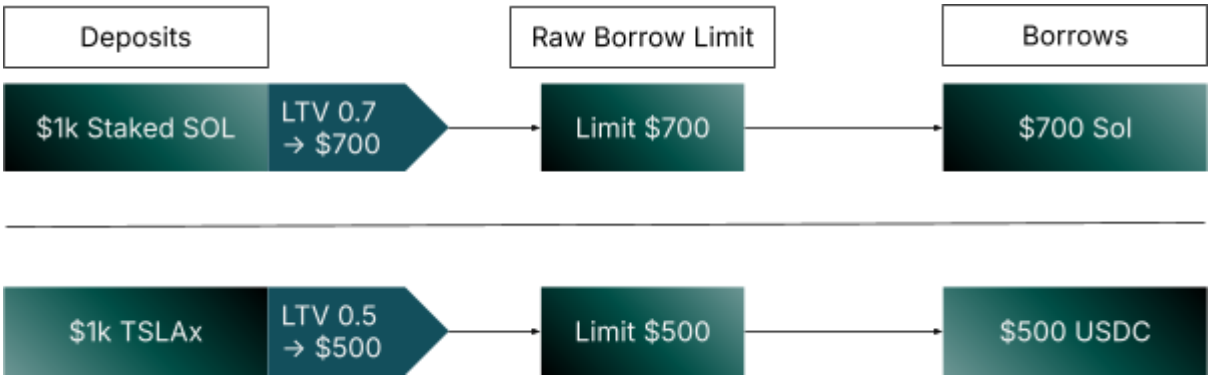
Poor capital efficiency

Fragmented liquidity reduces overall protocol efficiency, and significantly hinders users in their diversification efforts. This leads to low utilization across many markets, giving lenders poor yield, and makes the respective assets effectively unusable.

The Current Approach to DeFi Lending

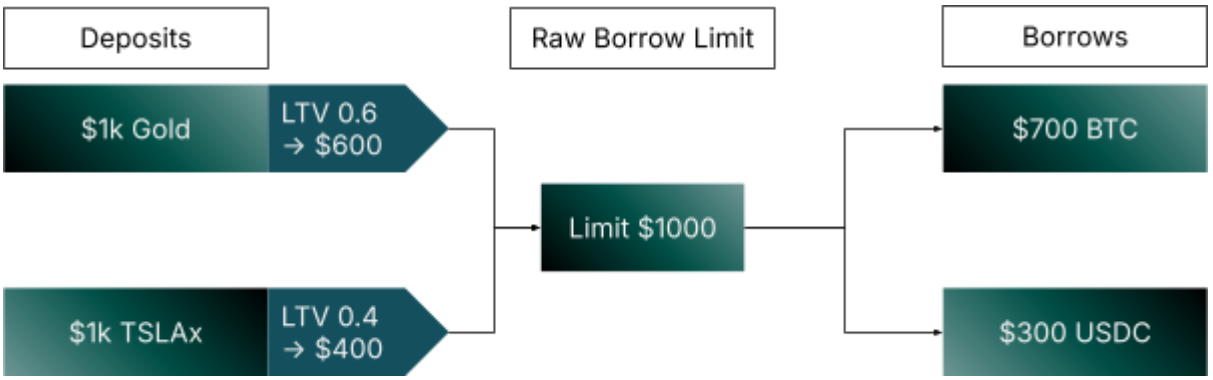
Vault Model (e.g. Morpho)

Vaults achieve good LTV accuracy for predetermined trading pairs and limit exposure against other assets. This is especially useful for high-risk use cases. Generally, LTVs are higher compared to other models.



Aave v3 Model

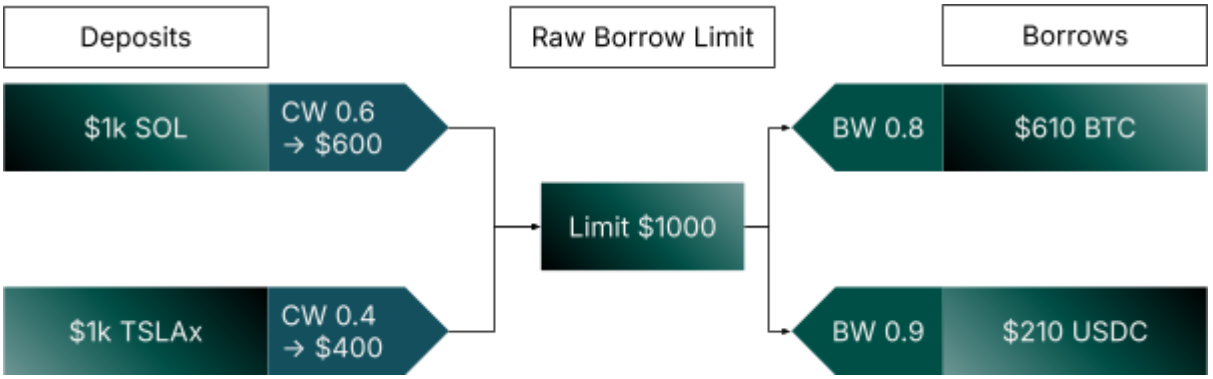
Onboarded assets are segmented into *markets*, which isolate different asset groups from one another. Aave uses a collateral-weighted LTV that gives a scalar borrowing limit. The specific borrowed asset or price correlations between assets are not considered.



To somewhat take correlation into account, e-mode can selectively boost LTVs when all collateral and debt assets are part of a shared e-mode group.

Kamino Model

Kamino splits LTV into *collateral weight* and *borrow weight*, where borrow weight is used to penalize borrowing capacity. E-mode is also available for specific asset pairings. It also uses *isolated markets* to limit risk exposure by users.



Conclusion

These examples directly show the current significant limitation: Because parameters are only tied to an asset in isolation, they cannot accurately reflect diversification or correlation effects. E-mode can somewhat map correlation between assets, but is only available for very specific asset pairings and does not work across more complex portfolio compositions and, more importantly, does not work for cross-market strategies. The last point is significant, because it means that not all collateral can be used to cover all debts! For example, a BTC collateral might not be able to be used to borrow SOL, making it useless in many portfolio strategies.

The Solution – Unified Portfolio Lending

Zodial replaces isolated markets with a comprehensive portfolio based risk model.

Users can:

- Lend and borrow against their entire asset stack rather than individual token positions
- Execute complex trading strategies including cross-asset hedges and sector-based positions
- Maximize capital efficiency through unified portfolio management
- Diversify risk across multiple asset classes

New Use Cases:

- Short RWA stocks against long crypto
- Hedge USD vs. EUR, MAG7 against gold, etc.
- Full diversification
- and many more.

Key Benefits

For Lenders and institutional LPs:

- Higher possible yield through improved capital utilization
- Better risk diversification across asset classes
- Access to a larger and more liquid market
- Transparent, portfolio-based risk metrics

For Borrowers:

- Higher borrowing power for the same collateral
- Sophisticated trading strategies in a single protocol
- Reduced liquidation risk due to portfolio-wide risk assessment
- Lower overall borrowing costs

Building a Unified Protocol

Pairwise Risk assessment

Most lending protocols use a conservative heuristic to determine borrowing capacity and portfolio health as detailed above for Aave and Kamino. Zodial uses precise, pairwise weights based on a 2D volatility matrix. We measure historical price divergence between all asset pairs, and get specific parameters for all collateral/borrow combinations.

How we think about risk and evaluate it

Before an asset is deemed suitable to be included in the protocol, it must satisfy the following conditions:

- minimum DEX liquidity and volume (to guarantee feasible liquidations)
- protocol / token maturity (to reduce manipulation and pricing risk)

For all eligible assets, the model ingests an extended, minute-level historical price dataset across all relevant trading pairs. For RWAs, the underlying asset is also included in the evaluation.

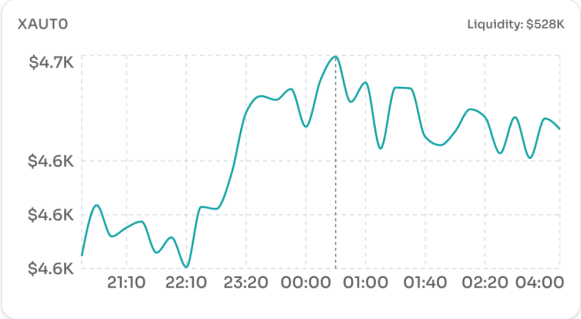
Liquidity and maturity determine a confidence score, which affects how conservative parameters are set and how large the price dataset window must be. For each eligible asset pair A, B, we compute the relative log move over a time window W:

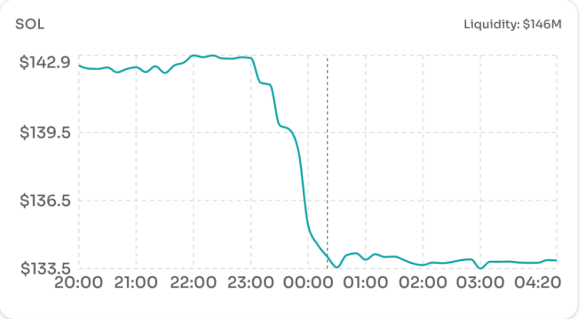
$$RLM(A, B) = ln(P_B(t) * P_A(t)) - ln(P_B(t - W) * P_A(t - W)).$$

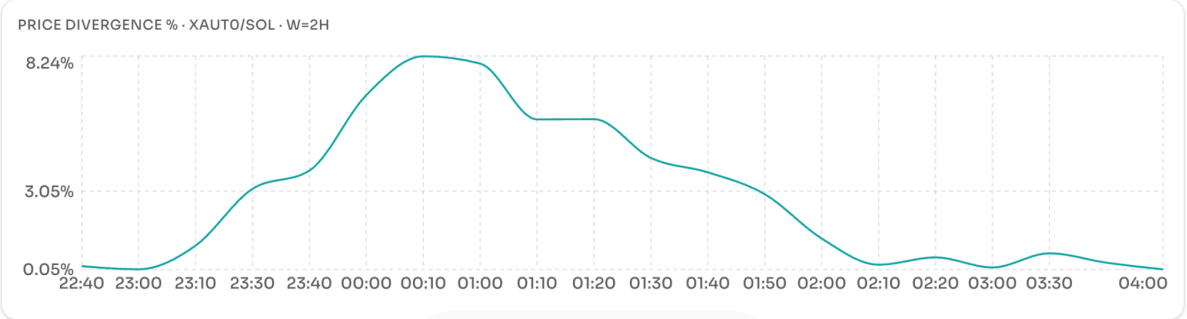
To capture volatility across market regimes, the model selected an observation window of 4h, based on DEX liquidity, market cap and maturity. For each asset pair, we identify the maximum observed

price divergence. From this, the model derives pair-specific parameters:

- Liquidation Threshold (LT): equal to max. price divergence
- Loan-to-Value (LTV): 98% of LT
- Liquidation Penalty: 50% of LT







Because risk is assessed per pair, closely correlated assets receive better parameters, while poorly correlated or crash–prone pairs remain conservative.

This unlocks possibilities for

- a single, unified market with higher asset utility
- improved capital efficiency for correlated and stable portfolios

To use the pairwise risk parameters to their full extent, the protocol needs a maximum capital flow algorithm which verifies that collateral can cover borrows for the given thresholds and market graph.

Capital Flow Optimization with Off-Chain Proofs

Pairwise risk parameters are only one side of the coin, but in isolation they do not meaningfully improve the protocol semantics. The more important question is: **How can the protocol determine how much of any given debt is covered by which collateral; and by how much of it?**

We can show that achieving this would yield a significant improvement for a users portfolio, using the starting example but now with pairwise LTVs and a maximum capital flow from collateral to borrows:

We can see that this approach can give us both a higher borrow amount and also significantly more headroom ($710 of the TSLAx collateral is unused!). The improvement compared to the current method becomes even more pronounced with more complex portfolios.

This approach is a known, solvable optimization problem for achieving maximal capital flow, but it is impossible to calculate on-chain because the needed compute power is orders of magnitude larger than provided by the blockchain. To still be able to use the best possible capital flow as a basis for the protocol, Zodial implements a split **off-chain/on-chain proof system**. The proof

system is powered by linear optimization algorithms and aims to move heavy compute operations to the client, with the contract as the proof verifier and enforcer of constraints.

Off-Chain Compute

The client solves the complex capital flow problem for any intended user interaction that negatively impacts health (e.g., borrow). As part of the computation, a *witness certificate* is generated, which contains the calculation inputs used by the client and constraints determined by the solving algorithm. The certificate allows for reconstruction of the capital flow without redoing heavy computation and it acts as a mathematical tamper-resistant proof that the portfolio is healthy for the given inputs.

For borrow, withdraw and leverage flows, the client only needs to provide a *feasibility certificate*, which attests that the portfolio is fully covered and also acts as a lower bound for the real health score. For liquidation, the client also has to supply an *optimal ("dual") certificate*, which provides the exact optimal capital flow and can thus prove that a user cannot be healthy under any circumstances.

On-Chain Verification

The contract handler for any of the above interactions expects both the in-flight interaction parameters and the generated certificate(s). The contract temporarily applies the wanted change to the portfolio, and then verifies the post-state portfolio against the provided certificate. If the certificate correctly matches, the transaction succeeds, or it is aborted if not.

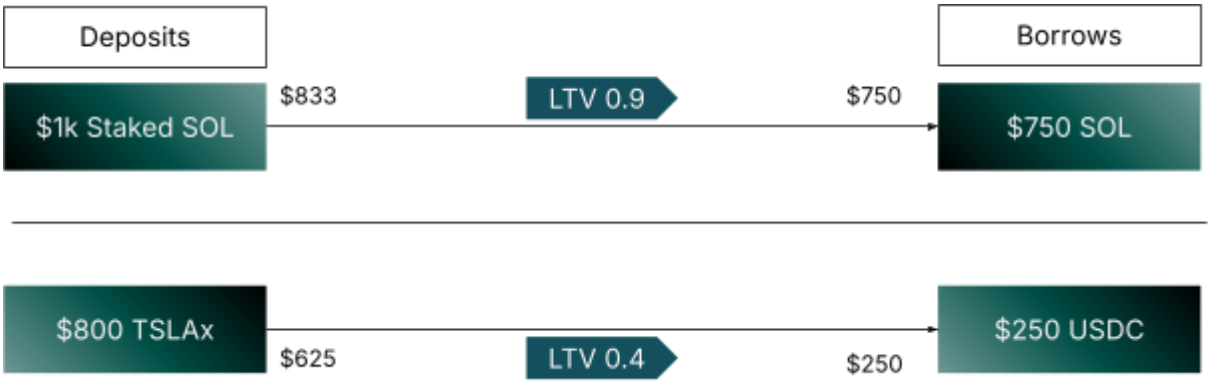
Read More

- Interior-point methods (Primal-Dual Method)
- Simplex Algorithm
- PDW method (3.4, Regression with High Dimensional Data)
- PDW method (2.4, Support Recovery Without Incoherence)

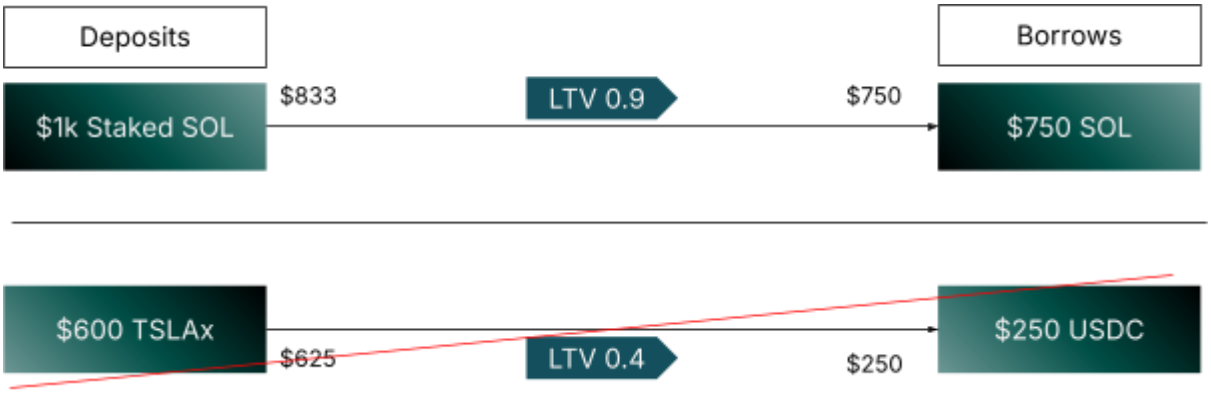
Avoiding Early Liquidations

A major flaw of the existing lending infrastructure is the isolated market approach. Since not every collateral can cover each debt, positions need to be overcollateralized more than theoretically needed, and do not cover each other.

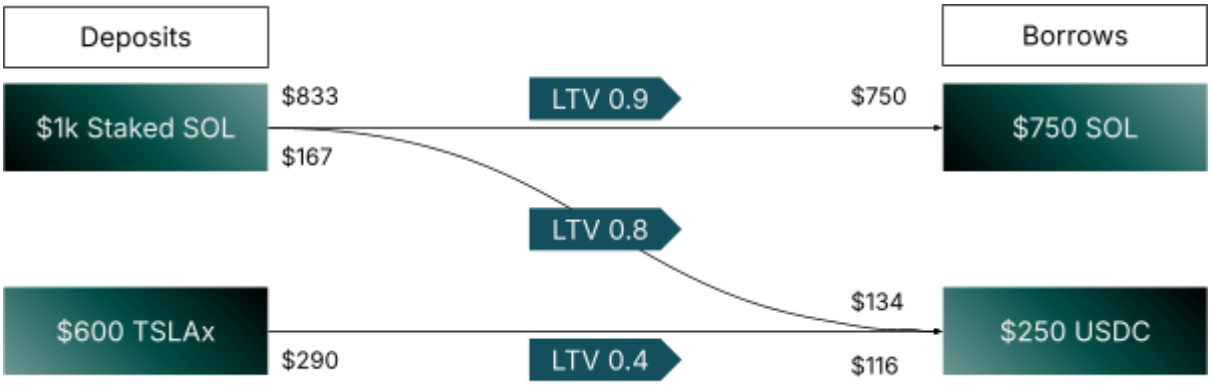
As a starting point, let's take this portfolio in an isolated market model:



If the valuation of the TSLAx collateral drops to $600, the position in the bottom isolated market will be liquidated, even though there is staked SOL headroom available:



In effect, the staked SOL collateral cannot cover this particular USDC loan, since it is part of a different market. With the unified approach, the whole portfolio is still covered:



Even a significantly larger price swing to a $300 TSLAx valuation would still be covered here.

Protecting the Market and Users from Price Attacks on Volatile Blue-Chip RWAs

Zodial uses a tried and proven method for handling RWAs that have closed market hours.
During market hours, token issuance mechanisms maintain the peg to the underlying asset through direct price alignment. When traditional markets are closed, users can still take actions based on the latest official closing price of the underlying asset.

While this may appear to create arbitrage opportunities from the perspective of the on-chain token price, payouts only occur if the asset's price movement exceeds the predefined Loan-to-Value (LTV) threshold. These thresholds are derived from extensive historical stock market data, analyzed across 92-hour periods and enhanced with a 10% safety buffer.

Conclusion

A unified lending approach powered by pairwise LTVs and optimal capital flow can significantly boost borrowing power for the same amount of supplied collateral and also protect against drastic price swings that can never be covered with the current approaches to DeFi lending. Achieving this required deep changes to the established LTV models and the introduction of a completely new proof system to offload complex math from the smart contract.

We believe that this system in combination with stablecoins, crypto and RWAs under a unified market will unlock the full potential of DeFi and bring significant growth to the lending ecosystem as a whole.