Morpho Blue Whitepaper

Mathis Gontier Delaunay

mathis@morpho.org

Paul Frambot

paul@morpho.org

Quentin Garchery

quentin@morpho.org

Matthieu Lesbre

matthieu@morpho.org

October 2023

Abstract

Morpho Blue is a noncustodial lending protocol implemented for the Ethereum Virtual Machine. Morpho Blue offers a new trustless primitive with increased efficiency and flexibility compared to existing lending platforms. It provides permissionless risk management and permissionless market creation with oracle agnostic pricing. It also enables higher collateralization factors, improved interest rates, and lower gas consumption. The protocol is designed to be a simple, immutable, and governance-minimized base layer that allows for a wide variety of other layers to be built on top. Morpho Blue also offers a convenient developer experience with a singleton implementation, callbacks, free flash loans, and account management features.

1 Introduction

1.1 Motivation

Traditionally, financial services rely on trusted institutions to process transactions and secure value. By allowing trustless code execution, blockchains and smart contracts challenge this paradigm. Decentralized finance (DeFi) aims to make financial services more open, efficient, and resilient than its traditional alternatives [10].

Two paths have emerged for building DeFi platforms: decentralized funds and protocols [9]. On the one hand, decentralized funds such as Compound [15] or Aave [19] are platforms similar to traditional funds, but they leverage onchain infrastructure and decentralized governance to function. While this approach offers a passive and liquid user experience, it has trust and scalability issues. For instance, decentralized funds rely on Decentralized Autonomous Organizations (DAOs) and trusted contractors to manage the platform's assets. They accomplish this by monitoring numerous risk parameters [8] and upgrading large smart contracts. DAOs are also not best suited for operational scaling,

and they can often become a bottleneck as the protocol grows. Additionally, due to their maintenance costs, these platforms necessitate fees from their users.

On the other hand, protocols such as Uniswap [3] are trustless and unopinionated smart contracts performing financial operations. This path has demonstrated remarkable resilience over the years. However, this primitive approach comes with usability tradeoffs at the protocol level. For instance, profitable liquidity provision on UniswapV3 [4] may require active and sophisticated position management.

What we will present is in line with the vision that DeFi should be organized in layers around trustless and open protocols, like the Internet. Onchain and offchain applications can be built on minimalist DeFi primitives to manage positions, handle compliance, or enhance usability for the user, for example. Depending on their needs, users can delegate some of their work to different layers. This model allows them to benefit from the efficiency created by the network effect around the primitive while remaining fully usable. A good example of this approach is UniswapX [5], which simplifies and optimizes the experience for UniswapV4 [2] traders who may have difficulty identifying the appropriate swap routing and managing MEV protection.

In 2023, Morpho Optimizer [11] has become the third-largest lending platform on Ethereum, with $1 billion in deposited assets. This initial platform was developed on top of Aave and Compound to enhance the efficiency of their interest rate model. However, developing the most significant platform built on top of decentralized lending platform helped us realize that they would never be sufficiently scalable, efficient, and resilient to reach the next level of adoption. As stated in the initial whitepaper [11], Morpho must metamorphose to become fully autonomous and enhance the current state of DeFi lending.

1.2 Introducing Morpho Blue

This paper introduces Morpho Blue, a new trustless and efficient lending protocol with permissionless market creation. Morpho Blue implements elementary, immutable, and isolated lending markets. On a market, suppliers deposit the *loan token* into the smart contract. On the other side, borrowers provide the *collateral token* to secure their loan whose Loan-To-Value ratio (LTV) can go up to the market's *Liquidation Loan-To-Value ratio (LLTV)*. Above this limit, the account will be eligible for liquidation. Assets are priced with the market's *oracle*. Borrowers pay lenders interest given by the market's *Interest Rate Model (IRM)*. To create a market, one must specify: a loan token, a collateral token, an oracle, a LLTV and an IRM. Both LLTV and IRM are chosen from governance-defined collections.

The Morpho Governance cannot halt the operation of a market or modify its LLTV, IRM, and oracle. However, it has the ability to expand the range of LLTV and IRM options available for market creation. Additionally, in each market, the governance can enable a fee ranging from 0% to 25% of the total amount of interests paid by borrowers.

In the remainder of this whitepaper, we first describe how the protocol externalizes risk management and how lenders can delegate this work to a permissionless risk management layer. The latter enables anyone to rebuild any user experience with any risk profile on top of a primitive, which features permissionless market creation and oracle-agnostic pricing.

Then, we explain specifics of the design. Notably, the minimalist approach allows for full auditability of the protocol and unlocks new levels of efficiency for interest rates, collateralization factors, and gas consumption.

Finally, we detail how the codebase of Morpho Blue improves the expressiveness of integrations and power users by utilizing notable code patterns such as a singleton contract, callbacks, free flash loans, and account management.

2 Externalized Risk Management

Removing the DAO risk management bottleneck is critical for DeFi lending to become more resilient and scalable. The current approach severely restricts the number of supported assets and confines users to a single risk-return profile[8].

A primitive protocol removes these downsides, but it may imply a more complex user experience and fragmented liquidity. In this section, we first explain how management layers can be rebuilt on top of Morpho Blue to re-aggregate liquidity and provide a passive user experience with diversified exposure for those who prefer it. Then, we describe how Morpho Blue externalizes oracle risk while still retaining the benefits provided by oracles. Finally, we outline how Morpho Blue eliminates the risk of bank runs and can continue running indefinitely without requiring any built-in management, regardless of market conditions.

2.1 Permissionless Risk Management

Morpho Blue is designed to be the foundational layer of decentralized lending. It is immutable, and the MORPHO governance cannot manage users' funds (see section 1.2).

The protocol is designed to leave the choices up to the users, notably by letting anyone create markets with any loan asset, collateral asset, risk parameters, or oracle. For example, one could create the market DAI backed by WETH as collateral with a LLTV of 90%, and using Chainlink[7] as the oracle.

While this flexibility offers a broader diversity of use cases, lenders must actively select the market in which they want to provide liquidity. This can lead to liquidity fragmentation and introduce complexities in risk management, which may deter lenders with less knowledge. To solve this problem, Morpho Blue is designed to serve as a basic building block that allows for the addition of more layers of logic. These layers can enhance the core functionality by handling risk management, or even compliance, and simplify the user experience for passive lenders.

Morpho Blue lending markets can be assembled to reproduce a multi-asset lending pool. For example, a vault could accept WETH from passive lenders seeking a risk-adjusted and liquid experience, then have a risk expert allocate deposits across various Morpho Blue markets where WETH is the loan asset. Here, the risk expert abstracts the complexities by selecting markets with appropriate collateral, LLTV, and oracles on behalf of users. In this case, WETH in the vault could be evenly allocated between WETH (stETH, 97%, Chainlink) and WETH (cbETH, 95%, Chainlink).
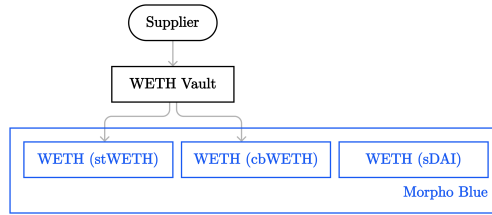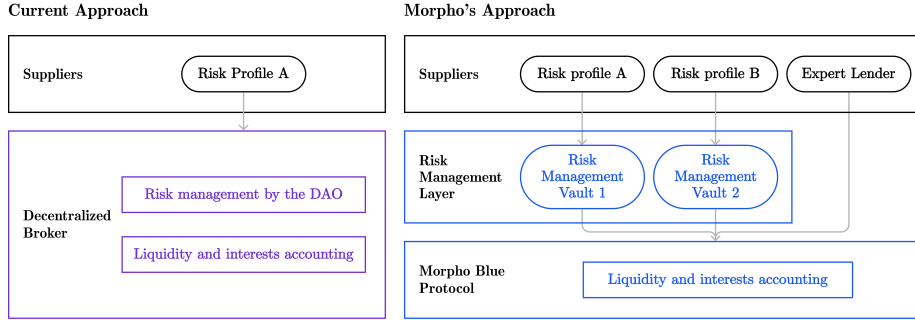

The example above illustrates how a Compound III ETH [14] experience can be replicated on top of Morpho Blue. It is possible to recreate any lending pool with any asset and any risk management method on this unique, trustless, and efficient primitive. As a result, it is also possible to build a vault similar to the AaveV3 WETH lending market.

With decentralized funds, when two platforms offer similar risks, their liquidity is completely segregated. However, with Morpho Blue, users with different risk profiles can share their liquidity on some common primitive markets. As a result, markets will benefit from deeper liquidity, creating network effects for all participants. Additionally, risk management solutions can easily compete, leading to better and cheaper products for end users.
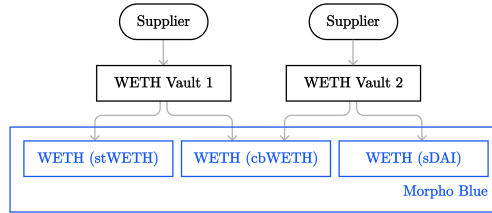
It is important to note that if the risk management of a platform built on top of Morpho Blue looses its users' funds, for either bad management or a technical issue, it will not affect the security of the primitive.

The following figure illustrates how Morpho Blue separates and modularizes risk management by separating it from the lending protocol.

Current Approach

| Suppliers | (Risk Profile A) |

Decentralized Broker
- Risk management by the DAO
- Liquidity and interests accounting

Morpho's Approach

| Suppliers | (Risk profile A) (Risk profile B) (Expert Lender) |

Risk Management Layer
- Risk Management Vault 1
- Risk Management Vault 2

Morpho Blue Protocol
- Liquidity and interests accounting

2.2 Oracle-Agnostic Pricing

For a lending protocol to operate efficiently, it must have an accurate notion of price. This price information is obtained by querying trading markets, whether they are internal or external to the protocol.

External price feeds, often called oracles, have various designs with different accuracy and security properties. For example, some oracles can provide frequent and accurate price updates, but they may be considered too centralized or manipulable to be at the core of a lending protocol.

To create more resilient lending primitives, some *oracle-less* protocols directly incorporated the pricing mechanics at their core. However, by doing so, the primitive has to handle both a trading and a lending mechanism simultaneously. This brings additional complexity, increasing gas costs and limiting auditability and security.

Morpho is dedicated exclusively to lending rather than trading. Its goal is to become the most open and efficient lending primitive while still operating in a trustless manner. This is why the protocol has an *oracle-agnostic* approach rather than an *oracle-less* one.

Morpho Blue has no oracle or trading mechanism built into the primitive. Instead, anyone can create a market by specifying an address that returns a price for the loan and collateral assets. Some markets may feature Chainlink or Uniswap oracles, while others could hardcode the price or use an innovative mechanism similar to Ajna's [17]. It is up to the users to decide which oracle they agree to depend on by choosing the corresponding markets to interact with. Lenders and borrowers could delegate this work to the permissionless risk management layer (see section 2.1), should this choice be deemed too complicated.

This way, Morpho Blue remains simple, trustless, and unopinionated while ensuring optimal efficiency for those who desire it.

2.3 Uncapped Markets

In current lending pools, the governance can set supply caps, constraining the total amount of a given collateral that can be supplied. This is notably used to control the exposure of lenders' funds to each collateral in pools where there are multiple ones. In addition, by ensuring that the size of the market stays below a certain threshold, supply caps can, for example, be expected to guarantee there is enough liquidity on exchange markets for liquidations. The latter is far from being ideal, though. For example, an external market composed of the same assets can freely grow, thus challenging these liquidity assumptions and making the guarantees of caps irrelevant.

Morpho Blue has no cap mechanism because it fully externalizes risk management. Instead, lenders are expected to achieve granular control over their exposure to different collateral by distributing their supplied volume across the different Morpho Blue markets. As explained in section 2.1, this work can be delegated to risk experts.

3 Minimal Lending Markets

In the nascent stages of DeFi, liquidity was an indispensable component. With few sophisticated actors, DeFi had to reinvent traditional finance mechanisms to make its markets usable. On the DEX side, constant function market makers (CFMMs) [3] were able to gather enough liquidity for emerging cryptocurrency markets by simplifying the market-making process to a "set and forget" design. On the lending side, Compound and Aave gathered multiple markets in the same pool, choosing common lending terms through the DAO and reinvesting collateral, meaning that the collateral itself can be borrowed. Although effective in bootstrapping DeFi liquidity, this design was forced to make a trade-off: prioritizing ease of use over efficiency and scalability.

DeFi is evolving. As the number and sophistication of actors increase, protocols have evolved to allow greater expressiveness. This not only enhances efficiency [16] for the user but, somewhat paradoxically, can also result in more streamlined logic and code.

3.1 No Re-Hypothecation

The first constraint of multi-asset lending pools is the fact that the markets must remain liquid at all times. Since collateral assets lent out may need to be liquidated, a consistent level of liquidity is required. Without it, it puts other markets at risk of bad debt. This means that the markets should not stay highly utilized for long periods of time. Concretely, it induces quite large spreads and interest rates to spike at high utilization.

In Morpho Blue, borrowers' collateral is not lent out to other borrowers but rather stays fully liquid on Morpho Blue's contract. As a result, the market's utilization can average higher, lowering the rate spread. Also, rates do not need to spike at high utilizations, providing more stability to borrowers.

3.2 Efficient LLTVs

In current multi-asset lending pools, there is typically one LLTV per collateral. In other words, the LLTV doesn't depend on the loan asset for a given collateral. However, reasonable models [6][13] for assessing the LLTV associated with a collateral asset also depend on the loan asset because one cares about the price of one of them quoted in the other. Consequently, risk managers of such lending pools must compromise between risk on uncorrelated loan assets and inefficiency on correlated assets. Aave introduced in its v3 [12] efficiency and isolation modes, which offer partial solutions to this problem. Similarly, Euler [1] introduced the concept of borrow factor.

Morpho Blue doesn't face this issue because LLTVs are defined for a market with one loan asset and one collateral asset. As a result, collateral ratios are improved for borrowers, usually leading to more interest generated for lenders.

3.3 Primitive Liquidations

When a borrower's LTV on a market exceeds the market's LLTV, the borrower can be liquidated. Anyone can perform a liquidation by repaying the account's debt and receiving the equivalent amount in collateral, along with an incentive factor, defined by the Liquidation Incentive Factor (LIF).

When establishing a liquidation incentive, there exists no definitive optimal solution. Rather, it is a fundamental trade-off between borrowers' costs, liquidators' incentives, and lenders' safety. Current protocols have different approaches to setting it. Aave and Compound have a fixed incentive per collateral set by governance, which tends to favor lenders. Euler [1] and Angle [20] have a health-dependent Dutch auction mechanism, meaning that the liquidation incentive increases when the health of the position decreases. This favors borrowers and disfavors lenders by reducing the liquidatable amount and the absolute incentive to liquidate above a certain health factor.

Regarding the proportion of the debt that can be repaid by the liquidator, or "close factor", there is a similar trade-off. Small close factors favor borrowers, and large ones favor lenders. Dynamic close factors, such as the ones allowing to liquidate only what is necessary to put the account back above water, reduce the immediate incentive and thus favor borrowers. In addition to that, as discussed in [18], fixed close factors can be bypassed by performing successive liquidations.

Morpho Blue opted for a static liquidation incentive factor per market because borrowers can reduce their exposure to the liquidation penalty — for example, by setting up an additional liquidation systems on top of Morpho Blue that are more favorable to them — while lenders can't do anything to improve on their guarantees. Its value depends on the LLTV of the market, according to the following formula:

$$LIF = \min(maxLIF, \frac{1}{1 - cursor \times (1 - LLTV)})$$

Where $maxLIF = 1.15$ and $cursor = 0.3$. This formula strikes a balance

between providing enough incentive to the liquidator and ensuring there is a sufficient margin to liquidate the borrower without accruing any bad debt.

With the same rationale, Morpho Blue favors lenders by having no close factor: when an account is liquidatable, its position can be fully repaid.

3.4 Minimal Codebase

Morpho Blue is an actual protocol. Hence, its contract is not upgradable, and the code is immutable. It allows anyone to anticipate and understand all of the smart contract's behaviors in advance. In addition, it makes the protocol truly trustless as you do not have to worry that the Morpho Governance can become malicious. It is crucial to notice that Governance cannot manage any funds, alter any market beyond setting a protocol fee, or create new types of markets by enabling new LLTVs or IRMs (see section 1.2).

The code is intentionally minimalist, designed for auditability while staying flexible enough to allow expanding features on top of Morpho Blue. The implementation is of around 650 source lines of code. Additionally, Morpho Blue's simplicity implies that it has less logic and a smaller storage footprint. This results in lower gas fees for interacting with Morpho Blue.

4 Enhanced Expressiveness

Morpho Blue implements several convenient smart contract patterns and attributes, aiming to enhance the capabilities of developers and power users.

4.1 Singleton

Morpho Blue's contract is a singleton, meaning all markets of a given chain live in one smart contract. This pattern simplifies interactions and reduces the gas consumption of platforms interacting with multiple markets of Morpho Blue, such as abstraction and delegation layers. It also concentrates liquidity for Flash Loans, described in section 4.3.

4.2 Callbacks

In the 'supply', 'supplyCollateral', 'repay', and 'liquidate' functions, which all perform a token transfer from the user to Morpho Blue, a callback to the user can be performed before the tokens are sent in the execution. In the callback function, one can do whatever they need to, including re-entering Morpho Blue. This notably removes the dependency on external Flash Loans and significantly reduces gas costs to perform advanced operations.

4.3 Free Flash Loans

Morpho Blue's singleton has a free flash loan function. Flash loans are loans that can be taken without any collateral if they are repaid in the same transaction.

Thanks to its singleton architecture (see section 4.1), flash loans have access to the liquidity and collateral of all markets simultaneously. This is typically useful in DeFi for liquidations, for opening and closing leveraged positions, and for arbitrages.

4.4   Account Management

Morpho Blue has an authorization system that enables users to grant permissions on their position to any address. An authorized address can borrow on behalf, withdraw on behalf, and withdraw collateral on behalf of the authorizer. Authorization can be managed in two manners: via a classic function call or via a message signature following the EIP-712 standard, similar to permit EIP-2612 for ERC20s. This feature allows notably for externally owned accounts to batch their interactions with Morpho Blue by authorizing a bundler contract. If needed, a more granular account management system can be implemented on top.

Acknowledgments

Disclaimer

References

[1] Euler white paper, 2021.

[2] Hayden Adams, Moody Salem, Noah Zinsmeister, Sara Reynolds, Austin Adams, Will Pote, Mark Toda, Alice Henshaw, Emily Williams, and Dan Robinson. Uniswap v4 core [draft], 2023.

[3] Hayden Adams, Noah Zinsmeister, and Dan Robinson. Uniswap v2 core, 2020.

[4] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. Uniswap v3 core, 2021.

[5] Hayden Adams, Noah Zinsmeister, Mark Toda, Emily Williams, Xin Wan, Matteo Leibowitz, Will Pote, Allen Lin, Eric Zhong, Zhiyuan Yang, Riley Campbell, Alex Karys, and Dan Robinson. Uniswapx, 2023.

[6] Samuel N. Cohen, Marc Sabate-Vidales, Lukasz Szpruch, and Mathis Gontier Delaunay. The paradox of adversarial liquidation in decentralised lending. August 2023.

[7] Steve Ellis, Ari Juels, and Sergey Nazarov. Chainlink, a decentralized oracle network, September 2017.

[8] Paul Frambot. It's time to talk about defi's risk management problems, 2023.

[9] Paul Frambot. The two paths ahead for defi: Decentralized brokers vs. protocol, 2023.

[10] Paul Frambot. What good can defi truly unlock?, 2023.

[11] Paul Frambot, Mathis Gontier Delaunay, Vincent Danos, Adrien Husson, and Katia Babbar. Morpho optimizer whitepaper, 2023.

[12] Emilio Frangela and Lasse Herskind. Aave v3 technical paper, January 2022.

[13] Chaos Labs. On aave's e-mode classes and their risk parameters, March 2023.

[14] Robert Leshner. Compound iii is live, August 2022.

[15] Robert Leshner and Geoffrey Hayes. Compound: The money market protocol, February 2019.

[16] J. Milionis, C. C. Moallemi, and T. Roughgarden. Complexity-approximation trade-offs in exchange mechanisms: Amms vs. lobs. *arXiv preprint arXiv:2302.11652*, 2023.

[17] Akash Patel, Ed Noepel, Gregory Di Prisco, George Niculae, Howard Malzberg, Ian Harvey, Joseph Quintilian, Matthew Cushman, and Michael Hathaway. Ajna whitepaper, March 2023.

[18] K. Qin, L. Zhou, P. Gamito, P. Jovanovic, and A. Gervais. An empirical study of defi liquidations: Incentives, risks, and instabilities. In *Proceedings of the 21st ACM Internet Measurement Conference*, pages 336–350, November 2021.

[19] Aave Team. Aave protocol whitepaper, January 2020.

[20] Angle Labs Core Team. Angle whitepaper, July 2021.