Arcadia Finance [Draft]

November 2023

Thomas Smets
Arcadia Finance
Brussels, Belgium
thomas@arcadia.finance

ABSTRACT

(To Do) Arcadia Finance introduces a novel on-chain architecture for collateral management of margined positions.

The overarching vision of Arcadia Finance is to build standardized on-chain infrastructure for collateral management, unlocking the capital in diverse DeFi assets, and establishing a comprehensive platform for managing collateralized positions.

As we anticipate the continued growth of on-chain tokenized assets and financial primitives, the importance of standardized and efficient collateral management becomes increasingly paramount. Without it, the full potential of these assets and financial primitives remains unrealized, hindered by protocol inflexibility and fragmentation.

Arcadia strives to enable higher capital efficiency for users, transparent risk assessment, faster go-to-market time for new protocols without compromising on security, self-custody and decentralisation.

KEYWORDS

Collateral management, DeFi, EVM

1 INTRODUCTION (TO DO)

This paper will explain the rationale why we are building the Arcadia Finance Technology Stack, and go over its technical implementation.

The Arcadia Financial Technology Stack is a set of on-chain, inter-linked financial protocols, centered around collateral management. They facilitate non-trusting peers to close financial contracts without the need of intermediaries.

It consists out of three protocols, each with distinct responsibilities and permissions:

- The Arcadia Registry.
- Arcadia Accounts.
- A Creditor contract.

2 TERMINOLOGY

Debtors and Creditors: We will often use the terms Debtors and Creditors throughout this paper, our definition is broader than the commonly accepted context within traditional debt arrangements. We use the term Debtor for any holder of a financial instrument that results in liabilities on the balance sheet (borrowers, option writers, payers of cash-settled futures contract or swaps...). While the Creditor refers to the entity to whom the liability is owed.

Open position: The size of the liability that a specific Debtor has with a specific Creditors.

Collateral: The assets pledged by a Debtor to a Creditor to cover the credit risk in case the Debtor would default.

Margin: The value of collateral assets that a Debtor must hold in a Margin Account to cover the credit risk of its Creditor(s). The margin requirements, are set by the Creditor. In general there are two types of margin requirements: Initial Margin (minimum value of collateral that must be held in the margin account to open a new position) and Maintenance Margin (minimum value of collateral that must be held in the margin account to keep an existing position open).

Margin Account: Our definition of a Margin Account extends beyond the conventional usage within Brokerage Accounts. The holder of a Margin Account not only has the ability to utilize and transact with the assets within the account (as is the case with a cash account or your standard crypto wallet), but can also incur liabilities against those assets. The margin requirements (initial and maintenance margin) are set by the Creditor.

3 HISTORY OF COLLATERAL MANAGEMENT

Withing the financial system, Collateral serves a primary function in mitigating the counterparty risks borne by Creditors, in case Debtors would fail to fulfill their financial liabilities.

3.1 Origin

Evidence of collateralized loans, also known as secured loans, can be traced back to at least 400 BCE in Ancient Greece [7]. In these early transactions, borrowers provided tangible assets as collateral to secure loans, laying the foundation for the concept of collateralization.

3.2 Current State

Over the past decades we have witnessed significant advancements in collateral management practices.

With the rise of complex financial instruments and the globalization of markets, the role of collateral has expanded beyond traditional lending. Collateral is now used to secure a wide range of financial instruments, including derivatives trading, margin accounts, and other sophisticated financial contracts.

The digitalisation of the financial system greatly improved the efficiency of the exchange and settlement of collateral. Reporting, margining and reconciliation processes could be executed on a daily basis instead of on a weekly or even monthly basis [9].

The emergence of blockchain technology and decentralized finance (DeFi) led to a new wave of innovation for collateral management. Blockchain has some excellent properties with regards to collateral management:

- With it's immutable and transparent ledger, collateral can be audited 24/7.
- Smart contracts enforce margin requirements real time on a 24/7 continuous basis.
- The atomic execution of transactions avoid expensive reconciliation processes.
- The atomic execution also enables optimistic execution of transactions (e.g. flash loans) which can greatly improve processes such as refinancing loans or even enable completely new financial use-cases.
- The permissionless nature of blockchain and Dapps (Decentralised Applications), combined with a shared state between all those applications, make different financial applications and assets composable and inter-operable by default.

It is no coincidence that some of the first blockchain applications with product market fit, were secured lending protocols. These early pioneers like Maker[10], Aave[11] or Compound[6] rely on collateralization as the only way to mitigate counter party risks and work with over-collateralized loans. As such they enable peer-to-peer or even peer-to-contract loans, without the need of any trusted intermediaries.

3.3 Collateral management in crisis

Collateralization, both in the traditional financial world and in DeFi, is not without its problems. Recent crises in both industries highlight the need for better collateral management infrastructure.

Bad collateral management, rehypothecation of collateral, opaque accounting practices of collateral, and outright fraud with collateralized assets, are all cited as root causes[4] behind the 2008 financial crisis. Following the crisis, a variety of major regulations were introduced (e.g. EMIR in the European Union, or Dodd-Frank in the USA). While these packages were successful in stabilizing the financial system, they have clear centralization tendencies[3]. The major beneficiaries of said regulations are the major established institutions, mandatory intermediaries for central clearing, central banks and the regulatory bodies themselves. This might paradoxically cement even greater systemic risks into the financial system.

In 2022 DeFi experienced it's own financial crisis. In a few months time, many of the ecosystem's key (albeit mostly centralised) players collapsed, and removed all liquid with them. Again bad collateral management, rehypothecation of collateral, opaque protocol mechanisms, and outright fraud with collateralized assets were at the root of the problem.

A recurring trend with protocols that imploded in 2021 and 2022 is that the lack of collateralization was obfuscated behind complex protocol designs and narratives. Some of the notorious examples are:

- Synthetic stable-tokens such as Gaia-USDf, Iron-Titan and Luna-Terra.
- Olympus and its forks relying on the (3,3) model.
- Protocols where the only utility of a token is to receive more of the token itself (animal yield farms, reflective tokens…).
- Unsecured loans by market makers and CeFi players.

DeFi protocols should focus more on collateralization, and less on Complex tokenomics that obfuscate who ends up paying when things go bad.

3.4 The Future?

The over-collateralized DeFi protocols however, operated remarkably well during the aforementioned crisis, even better than their traditional counterparts. This is well illustrated by some of the collapsed centralised entities, active in the space until 2022, that had both on- and off-chain liabilities. All on-chain Creditors were repaid in a timely and orderly fashion, as enforced by their smart contracts. While the lawsuits for the many off-chain Creditors are still ongoing (and probably will be for many years).

It is for these types of crises that liabilities are secured in the first place. These events further strengthened our vision that blockchain-based protocols have the potential to become the dominant infrastructure for collateral management. But before we get there, a number of Inefficiencies of in current DeFi protocols must be overcome, as we will discuss in the next Section.

4 COLLATERAL MANAGEMENT IN DEFI

4.1 General Principles

4.2 Inefficiencies

In the next sections we will highlight a number of inefficiencies, which need to be overcome before DeFi can be broadly adopted as the go-to infrastructure for collateral management.

4.2.1 Hacks and exploits. The major problem in DeFi today is the number of hacks and exploits, the estimated amount of funds lost in 2023 ranges from $400M to $1B. There are many security related practices the sector as a whole should improve on, but we want to highlight one problem.

Almost all DeFi protocols use over-collateralization in some way of form to manage counterparty risks between different user-groups. Lending protocols, perpetual protocol, Prime brokerage protocols, option protocols etc. all require some or all users to deposit collateral. While the nature of the financial contracts may be very different for each of these protocols, they share a great amount of common logic:

- Pricing of collateralized assets.
- Management (depositing, withdrawing…) of collateralized assets.
- asset-liability specific risk parameters and calculations.
- Margin calls and liquidations of risky positions.
- Settling bad debt.

Pricing of assets, management of assets and liquidation logic is complex, error prone and most mistakes easily lead to severe user losses. Today all protocols implement these redundantly, even for new versions of the same protocol. Not only is this very costly in development time, the core logic is rewritten and re-deployed time and time again, and with each new deployment, new bugs can be introduced.

Being able to build on top of battle tested code would benefit smart contract developers, protocols, users and the overall ecosystem.

4.2.2 Fragmented and isolated collateral. The average DeFi-user has collateralized assets fragmented and isolated across a multitude of protocols (do we have any numbers on this?), and many quality assets are sitting idle. While isolated margin positions have there benefits (they isolate risks), they are not capital efficient. Having the ability to use a portfolio of assets as collateral improves the capital efficiency for a number of reasons:

- The volatility of a portfolio of assets is always equal to, or lower than the weighted volatility of the individual assets. Or put different, assets losing in value can be compensated with assets increasing in value.
- Having less positions, with lower volatility, reduces the nu
- Depending on the correlation between collateralized assets, the Creditor might use less strict margin requirement.
- Debtors can use negatively correlated assets to hedge positions and limit liquidation risks.

Having a global shared state across applications and assets is often cited as one of the key advantages of blockchain over centralised financial infrastructures[8]. This should open up a whole new solution space for Debtors to manage collateralized positions, and might even enable a single Debtor to share its margin between non-trusting Creditors without intermediaries. Hence it is quite ironic that traditional brokers and clearing houses offer more advanced capabilities for cross- and portfolio-margined positions, compared to the state-of-the-art DeFi protocol.

Again there are again multiple underlying root causes why collateral in DeFi is still fragmented and under-utilized:

- As mentioned in Section 4.2.1, there is no shared collateral management layer, each protocol with collateral has their own non-standardized implementation.
- Protocols are build around specific assets types (eg. lending protocols for simple ERC20 or for AMM LPs, or for NFTs). Different asset types cannot be used within the same protocol to back a single position and emergence of new primitives/token standards requires migrations/new protocols.
- Blockchain is still a young technology, core non-financial infrastructure required for on-chain portfolio management (think Account Abstraction, intents or cross-chain messaging) is only recently developed.

Fragmentation of assets not only results in capital inefficiencies, it also contributes to a challenging user experience, more on that in the next Section (4.2.3).

4.2.3 End user complexity. End-user do not "want" to manage collateral, they want to optimize portfolio's to achieve a certain objective (e.g. increase yield, delta hedging, diversify exposure to different protocols...). Collateral management is a means to an end, it is not an activity most users enjoy doing.

End-user adoption will only increase outside of a niche bubble of tech enthusiasts if the technical complexities around collateral management are be abstracted away. Important note, abstracting away technical complexities should never come at a cost of hiding risks or relying on centralised and custodial solutions (as is to often the case).

As mentioned in the previous Section 4.2.2, the bad user experience is partly due to the fragmentation of assets and positions. Rebalancing portfolio's often require multiple transactions per asset and per position. Today the user has to execute multiple sequential transactions per asset, instead a single transaction that rebalances the complete portfolio. Let's take as example a user that wants to earn yield from his collateralized assets and get exposure to Liquid Staking Tokens (LSTs). Since LST protocols introduce an additional layer of risk, he wants to diversify risks over 5 different LST service providers. Assuming our user has wrapped Ethereum, he would need to do 10 transactions via multiple platforms (5 approvals and 5 swaps or 5 approvals and 5 staking actions). Rebalancing said portfolio, or depositing it as collateral, would require another 5 to 10 transactions. Not only is this time consuming, it also introduces additional operational risks, to name a few:

- Herstatt risk (settlement risk) due to changing markets before each leg of the action is settled.
- Increased risk of manual mistakes (fat fingers, bad slippage settings).
- Increased risk of falling victim phishing attacks on one of the platforms..

A second abstraction is to let users define what they want, and provide them with the information (the calldata) how to do it. Since most collateral management actions require interactions with multiple assets/protocols, this abstraction can only be achieved after portfolio's as a whole can be managed with a single atomic transaction.

At the time of writing this paper, the required infrastructure to enable both abstractions, is heavily debated within the broader ecosystem and multiple proposals are launched to standardize the infrastructure. Most notable are the proposals for Account Abstraction (e.g. EIP-3074 and EIP-4337) and for Intent based architectures (e.g. EIP-7521)

Both abstractions are already successfully applied (albeit in a somewhat non-standardized form) within DeFi by Decentralised Exchanges, NFT-marketplaces and their aggregators.

Our philosophy is that users should express what they want to do, not how they do it.

4.3 New Architectures

During the last months many solutions were proposed by different protocols and stakeholders on how to build a more robust decentralised financial system. Notable recent papers are for instance from Uniswap V4[1], Morpho[2] and Euler[5]. All mention similar concepts as the distinction between product and protocol, modularization of the protocol, oracle agnostic implementations and explicitly separating the logic of the protocol in different layers, where layers with different complexity evolve at different speeds.

Especially the last concept, to separate the logic in different layers, resonates with the long term vision of the Arcadia Finance team. Different Logic layers of the financial stack, with different complexities should have different life-cycles and innovation timelines. With the lowest most core component the slowest moving,

while the upper user facing layers must evolve and adapt quick in response ever changing markets.

A good practical example is uniswap V4, where Uniswap Labs implements the underlying core mathematical logic for CLAMMs (Concentrated Liquidity Automated Market Makers). Other teams can build in a permissionless manner on top of the Uniswap V4 protocol and develop feature rich and fast innovating new DEXs, without the need and risks of redundantly implementing the complex maths.

Also over-collateralized protocols would benefit from a similar architecture. A shared standardized and permissionless layer with battle tested logic for collateral management, on top of which Creditors build their application specific financial contracts.

Bringing back pristine focus to collateralization is exactly what we are doing with the Arcadia Financial Technology Stack. We believe that taking a collateral management first approach results in overall better DeFi protocols.

5 THE ARCADIA FINANCIAL TECHNOLOGY STACK

the Arcadia Financial Technology Stack is implemented for the Ethereum Virtual Machine (EVM) and consists out of three protocols:

- The Arcadia Registry.
- Arcadia Accounts.
- A Creditor contract.

General overview of the protocols, design requirements, permissions. - General philosophy: creditor is the maker, debtor is the taker. - Append only, no overwriting

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

6 ARCADIA REGISTRY

More details on requirements + technical implementation.

The registry is a modular and append-only registry for pricing logic and risk data of on-chain assets. Given the importance and nature of collateral, infrastructure to price collateral is of key importance that collateral should be: - Should be safe - Should be gas efficient - Should be liquid - Should be Should be resistant to price manipulation via flash loans - The size of the liability it backs, should be small compared to the liquid market size.

6.1 Many assets to one pricing

Creditor sets "routing".

6.2 Modular pricing logic

Append only

6.3 Risk Mitigation

It is impossible to guarantee that every module will always be bug free. A protocol where new pricing modules can be appended, but that relies on the assumption that all bugs will be caught before deployment of each module, is bound to fail. A bug in a single module should not lead to the end of the entire protocol and to all protocols build on top of it.

The probability that bugs might occur in a module at some point should be taken into account in the protocol design. This consists of three steps: impact mitigation, impact isolation and module replacement.

Risk parameters should be granular enough to be able to capture the smart contract risk for novel modules. Different Creditors should be able to decide when they enable their debtors to use assets priced by a certain module as collateral. And when they decide to enable the module, set upper boundaries to the overall exposure to said modules. As such, if one module is faulty, it should be possible to mitigate it's impact.

After a bug is identified

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

7 ARCADIA ACCOUNTS

7.1 Multi-collateral

7.2 Token Standard Agnostic

7.3 Margin Accounts

7.4 Account Abstraction ready

7.5 Flash Accounting

7.6 Intent ready

7.7 Automated Asset Management

7.8 Upgradeability

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Figure 1: Example of an image.

8 ARCADIA CREDITOR

8.1 Generalised Creditor

8.2 Composable

8.3 Risk Management

8.4 Accounting Liabilities

8.5 Liquidations

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

8.6 Arcadia Lending Pools

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

9 SUMMARY

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

REFERENCES

[1] H. Adams, M. Salem, N. Zinsmeister, and et al. 2023. Uniswap v4 Core [Draft]. Draft.

[2] Mathis Gontier Delaunay, Paul Frambot, Quentin Garchery, and Matthieu Lesbre. 2023. Morpho Blue Whitepaper. (2023). https://github.com/morpho-org/morpho-blue/blob/main/morpho-blue-whitepaper.pdf

[3] J. Gregory. 2014. *Central Counterparties: Mandatory Central Clearing and Initial Margin Requirements for OTC Derivatives*. Wiley. https://books.google.be/books?id=DpXqAwAAQBAJ

[4] Martin Hellwig. 2008. The causes of the financial crisis. In *CESifo Forum*, Vol. 9. München: ifo Institut für Wirtschaftsforschung an der Universität München, 12–21.

[5] Euler Labs. 2023. Protocols vs Products. (2023). https://www.euler.finance/blog/protocols-vs-products

[6] Robert Leshner and Geoffrey Hayes. 2019. Compound: The money market protocol. *White Paper* (2019).

[7] P. Millett. 2002. *Lending and Borrowing in Ancient Athens*. Cambridge University Press. https://books.google.be/books?id=0IriOXQSe5QC

[8] Fabian Schär. 2021. Decentralized finance: On blockchain-and smart contract-based financial markets. *FRB of St. Louis Review* (2021).

[9] M. Simmons. 2019. *Collateral Management: A Guide to Mitigating Counterparty Risk*. Wiley. https://books.google.be/books?id=DMOKDwAAQBAJ

[10] Maker Team. 2017. The dai stablecoin system. (2017). https://makerdao.com/whitepaper/DaiDec17WP.pdf

[11] Harry Thornburg. 2020. Aave protocol whitepaper v1. (2020). https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf

DISCLAIMER

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.