Dolomite ...  **Try HackMD**(https://hackmd.io?utm_source=view-page&utm_medium=logo-nav)

Dolomite Money Market Review

May 10, 2024

Prepared for Contango Protocol

Conducted by Richie Humphrey (devtooligan)

About the Contango Dolomite Money Market Review

Contango builds perps by automating a looping strategy, also known as recursive borrowing and lending. This is achieved using spot and money markets.

This review focused on the `DolomiteMoneyMarket` contract, a new adapter for Contango which enables depositing and borrowing with Dolomite.

About Offbeat Security

Offbeat Security Labs, LLC is a boutique blockchain security company specializing in complex and novel DeFi projects. Our mission is to elevate the blockchain security landscape through innovative, collaborative, and unconventional solutions.

Summary & Scope

The dolomite (https://github.com/contango-xyz/core-v2-private/tree/bcf5ad72fba8baae087fe6fbf070fc1c0cc7b7c4/src/moneymarkets/dolomite) folder of the `core-v2-private` repo was reviewed at commit 557f61af27ccd69b0a71d74c2a7bf3b7de6df30b.

The following one contract was in scope:

- src/moneymarkets/dolomite/DolomiteMoneyMarket.sol

The client has also requested that we document any assumptions implicit in the code which we encounter during our review.

Summary of Findings

During the course of this review, we identified an error in the Dolomite documentation (https://docs.dolomite.io/developer-documentation/dolomite-margin-glossary) which indicates the `otherAddress` field is not used for withdrawals or deposits. However, the client has reported that this is incorrect and it breaks all tests if it is removed.

No other findings were identified.

Additional Recommendations

In the `__withdraw` and `__deposit` functions there are many fields in the `ActionArgs` argument which are intentionally not set. This has the effect of setting those fields to 0 or in the case of an enum, setting the top enum value.

To better inform future development, consider either explicitly setting those fields to the desired value, or adding comments that explains and exposes the intentionally unset fields.

In addition, add a comment referencing the error in the Dolomite documentation to avoid confusion in the future.

Code Assumptions

Assumptions noted:

1. Native tokens will not be used to interact with Dolomite.

2. A position requiring the use of an isolation vault will be correctly indicated in the `positionId` provided to the `_initialise` function.

3. Dolomite vaults are trusted with uncanceled, maximum approvals.