Frankencoin

Security Review

Ethan Bennett Darklinear Solutions

About Darklinear Solutions

Darklinear Solutions leverages years of expertise in smart contract and software engineering to provide unrivaled security reviews for blockchain applications. Learn more at darklinear.com.

Introduction

Frankencoin is a stablecoin pegged to the Swiss franc and forked from Liquity. This review consists of issues discovered during the course of Code4rena's Frankencoin contest in April 2023. It does not represent a full and exhaustive audit of the protocol.

The findings described below are classified according to Code4rena's standards.

Finding

Unique: No other competitor identified this issue

Auctions fail to account for network and market conditions

Severity: Medium risk

Context: MintingHub.sol#L199

Description: Under certain extreme, but inevitable, network conditions, auctions will not be effective in covering the bad debt of a challenged position. Worse, certain position parameters under these conditions can lead to extremely small bids winning large amounts of collateral. More details follow in the next section, but it should be noted that this same design oversight was responsible for almost destroying Dai in March of 2020 — the closest MakerDAO has ever been to utilizing its emergency shutdown module.

Proof of concept: When the Ethereum network becomes highly congested, the price of gas can skyrocket to incredible levels. During times like these, users of the network will limit their activity to only the most urgent matters — in the case of March 12th, 2020, for example, the only people paying the exorbitant network fees were rushing to exit their positions as the price of ETH (and everything else) began to free fall.

On that day, MakerDAO's collateral auctions were slipping by unnoticed, as the bots that would typically compete in the majority of these auctions saw failing transactions, hit cost limits defined by their owners, or were simply deactivated. An attacker noticed them, however, and began winning auctions on liquidated collateral with bids of zero ETH.

This exact vulnerability exists in the Frankencoin system, and it can be exploited under exactly the same circumstances. If a challenge only has a single bid when the challenge period ends, and that bid is near zero, the bid will still win the collateral regardless of how much it is actually worth.

At first glance, Frankencoin developers might be tempted to believe that the dynamic challenge period on its positions will allow for the system to rely primarily on auctions that can outlast abnormally volatile days. In practice, however, this is unlikely to be true, since "safe" positions will likely end up

with very short challenge periods. This is unavoidable, because the vast majority of ZCHF will be backed by these types of collateral, and the system risks carrying untenable amounts of bad debt ever more the longer these challenge periods are extended. And extending these windows does not actually solve the problem anyways, since the bad debt cannot be covered until they end.

Consider, as well, that Frankencoin has a significant additional barrier to liquidating its positions when compared with MakerDAO: challenging requires collateral. If huge swaths of positions against a highly trusted collateral type all violate their liquidation prices concurrently, the amount of capital required to challenge all unsafe positions at once is unlikely to materialize quickly. This will lead to a severe loss of confidence in the ZCHF peg, as the system's bad debt balloons, auctions clear for pennies on the dollar, and large, undercollateralized positions remain unchallenged. The peg likely could not withstand the ZCHF panic selling that would doubtlessly occur alongside this.

In fact, this vulnerability does not even require a malicious actor to make the protocol insolvent in market conditions such as these. Since a challenge with no bids will determine the collateral to be worthless, the protocol will fail to liquidate any collateral from some or all of its unsafe positions.

Recommended mitigation: The auctions should be converted to "dutch auctions." This simply means that, rather than starting from zero and accepting the highest bid, the auction should start above the liquidation price and gradually decrease. This will prevent any challenges from ending with winning near-zero bids.