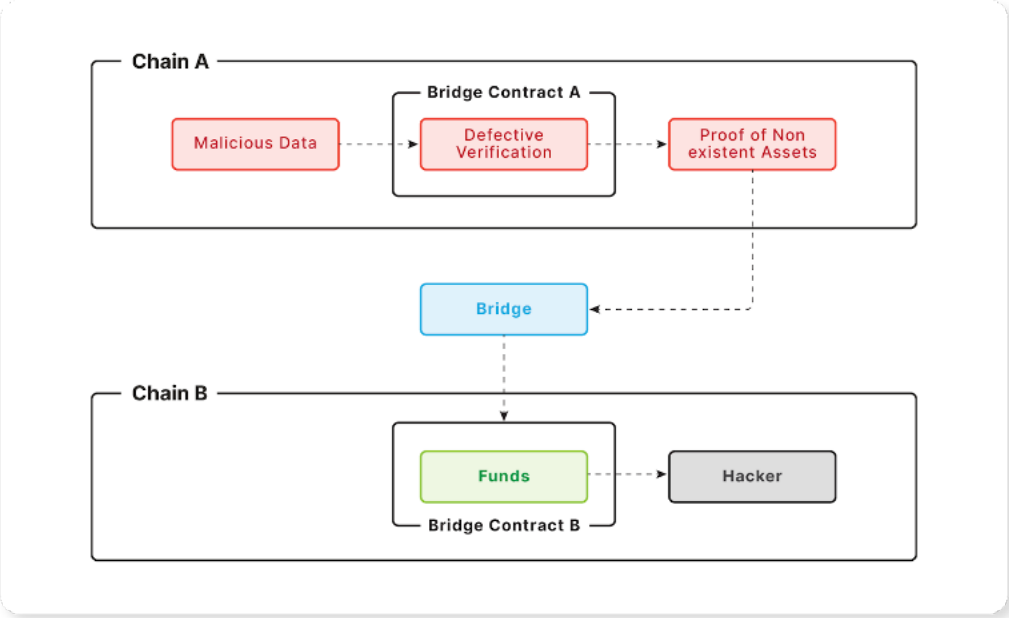
A word on Cross-Chain Bridge Risk

@0xMT brought up cross-chain bridge risk and how it relates to adding an asset such as $FTM to Anchor. The Fantom Foundation, along with many other prominent projects, are reliant on Multichain (formerly Anyswap). Multichain is currently our cross-chain swap partner for DOLA. Others, like Abracadabra, use chain-specific bridges (e.g. Arbitrum official bridge for Arbitrum, Avax bridge for Avalanche, etc). In 2022 alone, four major attacks have already occurred on cross-chain bridges – QuBit, Wormhole, Meter.io, and, most recently, Ronin.

To better understand these incidents, we need to know what a bridge is and how it works. In short, a bridge moves assets from one blockchain to another. A cross-chain transaction can work as follows:

- A user "deposits" tokens into a "bridge contract" on one chain and generates a proof specifying the required cross-chain information (e.g., the number of tokens to be withdrawn and the recipient address).
- The bridge verifies the proof and, on the target chain, the user can “withdraw” the tokens from the bridge contract.

In the three recent incidents, attackers injected spoofed data, bypassed the verification, and withdrew the corresponding tokens on the target chain to a specified address. Below is a depiction of a common attack vector on Bridges.



For more detail on the specific exploits, refer to this article published by auditors Certik: https://www.certik.com/resources/blog/technology/cross-chain-bridge-attacks-explained

@0xMT performed his own research on the topic and presents his findings below:

I skimmed through the audit reports of Multichain/Anyswap conducted by Trail Of Bits and Peckshield, and while the found issues were mitigated, I wouldn't say they inspire confidence. The peckshield report only raises one important issue, which is that of an EOA account controlling the minting functions. This is hard to avoid in bridging contracts, and the EOA in this case is a MPC derived private key. Essentially an off-chain multi-sig. The real question about the security of this set-up, is the nature of that multi-sig. We've all heard of the recent Ronin bridge exploit, where 5 of 9 keys were compromised. I wasn't really able to find any information on Multichain's SMPC Network in their docs, so it's hard to estimate how distributed it is.

The Trail of Bits audit seems more damning, with finding multiple errors in their underlying cryptography, which could be used by an attacker to essentially mint tokens. Now I'm no cryptography engineer, but one thing I remember from my courses on the subject, is just how easy it is to make a seemingly innocuous mistake, that leaks enough information about the secrets involved to be able to suss out how to forge signatures over time. Trail of Bits is of course an excellent security company, and they've helped Multichain/Anyswap fix the problems. The audit report was conducted in November 2021, with the updated report and their fixes being published Feb 22 2022.

From Trail of Bits Audit:

> The significant number of high-severity issues discovered during our review are indicative of an immature codebase that has room for improvement. These issues largely stem from incorrect protocol implementation and improper data validation. Several of these issues affect critical areas, and we suspect that similar issues are present elsewhere in the codebase. Therefore, we recommend that AnySwap focus on protocol implementation and data validation moving forward.

So how does this relate to adding $FTM and other similar assets to our Anchor Money Market? The worst case scenario is a similar situation to the recently Wormhole hack, where a flood of fake FTM tokens is used to drain whichever DeFi protocols will take them in exchange for anything else of value.

In that scenario, we have options to address this risk:

- We can limit the damages by implementing a hard cap on the amount of FTM that Anchor can absorb. This in general is good policy to mitigate potential damage from bridge failures.
- Alternatively, If code permits it, a maximum FTM delta per {time period} could be instituted, along with a governance circuit breaker, to mitigate potential losses.
- A hardcap that's manually increased as more FTM is added to anchor mitigates most of the damage, as a hacker would only be able to steal (Hardcap - Supplied FTM) * LTV ratio worth of liquidity. Though having to continuously raise the cap might get a bit tedious.

Such measures don't eliminate all risk. An infinite mint attacker could potentially fill up to the hardcap, tank the price by $FTM 10%, then liquidate themselves and do that all over. Prompt governance action would still be needed in the event of a hack, though such an attack would be specifically targeting Anchor and its fair to assume there are bigger fish in the sea for hacker with infinite FTM. The guardian role allows for a pause but not unpause of a market in case of emergency without governance.

Outside of an infinite mint exploit and given FTM's current MCap, it's unlikely FTM's price would be permanently affected by a Multichain hack, so long as there are other working bridges between FTM and ETH. It should also be noted that If Multichain were exploited the foundation would almost be forced to replenish at least $FTM if not more assets. Multichain is the #1 source of TVL for Fantom and largest recipient of their grant by far.