Inverse <> Beanstalk Partnership Recommendation

In short, Beanstalk issues a algorithmic stablecoin called $BEAN, pegged to 1$. It's an algorithmic stablecoin, variation of bDollar, mDollar, Tomb.

General thoughts on $BEAN:

I question their survival odds. AlgoStables never have a good system to burn supply. I honestly doubt it's sustainable, these algo stables never have a good system to burn supply. No algostable has worked so far, Bean doesn't strike me as something different.

What you have is an uncollateralized "stablecoin" that's only purpose is farming with high APY, lacking an effecting balance sheet and shrinking mechanism. It has no use case outside of its own ecosystem. It's a reflexive ponzi (maybe less than the others mentioned – since gov token $STALK must be burned to retrieve your LP).

It may have a better design than Tomb or bDollar, but the reason it's still around is because it hasn't reached the "implode" phase yet. Their mechanism to hover back to the 1$ peg is by being able to buy debt that pays you more Beans when the price repegs. This has been tried time and time again and will always fail because regardless of how much people "burn" to get this debt you still need someone to bid the price. The real supply is always growing (adjusted for pending debt) and so you can never support a drop in demand. What will happen in the implode phase is that existing holders of the stablecoin burn it in order to get more when it repegs but there's nobody to actually take the risk and buy in (new capital), so it never repegs. Leading to a disbelief phase and eventually It ends up trading close to 0.

Beanstalk has survived to this point because there was money bidding it to go back to peg. The debt adjusted supply never shrinks. When the protocol mints a new bean, its split 50/50 between LP and creditors. What would an LP do in that scenario? Either get out of the pool because of the huge price risk or sell the BEAN they got to lower the cost basis. Each debt cycle is bigger than the last, it has no way to deleverage itself. So eventually you reach a point where it implodes and never recovers. When that happens is unknown, could be at a circulating supply of 50M, 100M, 1B, etc, but it is guaranteed to implode.

A point to address – there is always a price point where someone in the world is willing to take the risk to bailout the protocol if the reward is high enough. But in reality there

isn’t because the situation might be such where the repeg is unattainable (e.g. BDO could’ve been purchased at $0.10 way back when. If it had ever gotten back to the peg, your return on investment would’ve been great. Instead BDO price went to $0.01). In short, why would anyone bid it to the upside when all the debt being accrued is baggage to the protocol. Debt accrued caps your upside whilst you still have a long downside to go.

Another point – there is no interest in leaving the LP because since the gov token is earned slowly over time, and when you withdraw your LP you need to burn all earned stalk, the opportunity cost the withdraw increases over time. - Gov token isn't something you can trade like shares of bdollars - Opportunity cost grows over time so people don't leave the silo.
To that I say:

- If you have your capital at risk in a possible final depegging event the last thing you think about is the stalk you've accrued overtime.
- It dissuades new users to become LPs compared to someone who's been there for months. The later you're into the cycle the more risk you carry

$BEAN, $BDO, etc, type Algostable have clear flaws. The best case of an algo stable working (at least for the moment) is UST. Which of course has its own risks.

Update: April 17, 2022

https://twitter.com/FrankResearcher/status/1515693895887294466

Big exploit this morning. We turned down a partnership with them last month. Looks like a governance attack it. They didn't have any sort of delays for governance implementation, so it was possible to acquire majority ownership of governance with flashloans and push a BIP, all in the same block. In this case the governance token wasn't transferable and could be acquired by depositing into the Silo, so it was much easier to acquire the majority of the governance stake. Safety measures for such an attack: Have your governance token be illiquid enough so that even if someone goes ahead and flashloans and buys all of the tokens that can be bought they still can't pass a proposal. And also adding delays (like we have for our governance process)