TLDR

: We describe a stablecoin design engineered to effectively manage contentious chain forks.

Co-authored by @edmundedgar and @josojo

Why its useful to develop forkable stablecoins

There are two major benefits to developing and adapting forkable stablecoins:

1. Forks may break stablecoins, or if forks can't happen that weakens Ethereum's security

Economic forks are challenging for stablecoins collateralized by crypto-native assets: The value of the collateral is approximately split among two chains, while for each chain the face value of the stable asset they represent appears on both. A chaotic situation arises where depending on the ultimate ratio of the collateral value, the value of the stablecoin might double (if collateral on both chains preserve enough value to avoid liquidation) or disappear altogether (if neither does). If we expect only one fork to avoid liquidation, a user putting up collateral must account for the prospect that the part of their value they hold on the losing chain will be liquidated.

The result is that a fork will potentially do lethal damage to stablecoins as currently designed. Alternatively, it may be the fact that this damage would occur makes contentious forks impossible, which weakens the security of the chain, underpinned as it is by subjectivocracy.

1. Enable a more secure oracle for the stablecoin:

If a stablecoin can actually handle forks in a relatively clean manner, this would allow for deploying them on forkable systems: This opens the door for new, more secure oracle designs that use subjectivocracy. Elsewhere we discuss how these new oracles could be enshrined into a forkable L2. These new oracles would then improve the stablecoin itself, as oracles are a fundamental building block for stablecoins.

We propose a design that rebases the stablecoin token on each side of the fork in line with the collateral, preserving the total value of the stablecoin and avoiding instant liquidations after the fork.

Design

Assumptions:

For this write-up, we assume that there is an oracle for the stablecoin that provides the price between the forked collateral. In the system, we propose here whereby the forkable stablecoin and its collateral are living on a forkable L2, the price ratio can be determined on L1 via an auction/trading without further assumptions on a working oracle.

Solution

The proposed stable token works quite similarly to RAI or DAI. Stable tokens, called forkable DAI (FAI), are created by opening CDP positions, and interest is paid through a slight, continuous change in the FAI token's value compared to the dollar.

If the chain is forked, each child chain will receive the collateral ratio price via the oracle. The FAI value will be rebased based on the forked collateral ratio. For example, if the ratio split between the branches is 30% to 70%, on the 30% branch, the FAI will be rebased to hold only 30% of its value, and the remaining 70% will be held on the other branch. If the overall market cap of the underlying token of the chain (the sum of both child tokens) does not change during the forking process, all CDPs should be well covered on both chains.

After the fork, each FAI holder has the option to reunite their split FAI value by trading FAI^1 from the first branch for FAI^2 from the second branch. This ensures that the promise to each customer to hold roughly $1 of value is honored during the forking process. Subsequently, although the value of the collateral is likely to change both in absolute terms and in relation to the collateral on the other fork, the value of each fork of the stablecoin should hold its (rebased) value by the normal mechanism.

Risks and limitations

- If a user has locked their FAI in a long-term commitment contract and cannot exchange it from a losing branch, they may effectively lose value. For example, if a branch initially holds 5% of the overall market capitalization and is later abandoned, causing its newly underlying token to be worth 0, then the CDPs can no longer remain active and the FAI will be liquidated. This results in a 5% loss of value for the user since the original value of FAI was rebased by 5% during the forking process. The remaining 5% of the value will be lost once the claim is available to the customer, as all CDPs will be liquidated, and the collateral on that fork will be rendered worthless. This loss scenario only occurs when a minority fork initially has value but is later completely abandoned. Historical data from forks such as ETHC, ETHW, and BCH show that they usually retain some valuation for a considerable amount of time, allowing stablecoin

owners ample time to leave the fork with the correct valuation of their stablecoins. This risk can also be mitigated by setting a minimal cut-off beyond which all value should be assigned to the majority fork. In the past stablecoins have survived the creation of minority forks worth 5% or so of the value of the majority fork without major disruption for a reasonable time frame.

- Although this system protects the value of a stablecoin held by a user, some contracts that expect to have entire face value in the stablecoin token will need to handle additional complexity. For instance, if an unforkable real-world asset is priced in the stablecoin, the price denominated in the stablecoin will change. We can make this process easier for contracts to handle by giving the stablecoin the ability to report the price at which it was rebased.

Overall we think that this stablecoin design is very promising as it is the first stable coin design that is forkable and allows subjectivocracy to protect the oracle and thereby eliminate one major risk factor of usual stablecoin designs. We are curious about your input or other forkable stablecoin designs from the community!