Response to Consultation Paper

Draft Regulatory Technical Standards on information for application for authorisation to offer to the public and to seek admission to trading of asset-referenced tokens and Draft Implementing Technical Standards on standard forms, templates and procedures for the information to be included in the application, under Article 18(6) and (7) of Regulation (EU) 2023/1114

Question n. 4: Do you consider that the information requirements about the policies and procedures on the composition and management of the reserve of assets, as well as on the custody and investment of the reserve of assets are sufficiently clear and comprehensive?

To Whom It May Concern,

We appreciate the opportunity to provide input in response to the public consultation paper about the policies and procedures governing reserve requirements for asset-referenced tokens (ART) issuance. Our imperative in this response letter is to draw clear distinctions between asset-referenced tokens issued under the purview of centralized entities from those digital assets that emanate from decentralized ecosystems.

ARTs or stablecoins pegged to stable reserves, can be bifurcated into centralized and decentralized constructs. On one hand, centralized stablecoins, exemplified by Tether (USDT) and USD Coin (USDC) derive their stability from fiat reserves safeguarded by centralized entities. This ensures a close alignment with the pegged fiat value.

Conversely, decentralized stablecoins, like DAI and crvUSD, function on a different premise. Anchored not to fiat, but to crypto assets in smart contracts, they champion a trustless, transparent architecture. The operational autonomy, governed by pre-determined protocols, reduces centralized intervention. Yet, there are challenges such as the volatility of backing crypto assets. They also grapple with liquidations — emergency sell-offs when collateral is scant. This can exact hefty costs on users, either through collateral losses or steep fees. Additionally, their over-collateralization model demands a blockchain-integrated price oracle, crucial for orchestrating liquidations and safeguarding the system's financial health.
DAI's stabilization mechanism is reviewed in our recent asset risk assessment:

- DAI originally relied solely on Ether as collateral but has evolved to incorporate real-world assets, diversifying its collateral portfolio. This provides stability during crypto market volatility.
- A key component is the DAI Savings Rate (DSR), which incentivizes holding DAI by offering interest rates set by Maker governance. The DSR helps balance DAI supply and demand. Gradual rate adjustments maintain competitiveness while avoiding sharp supply/demand imbalances.
- Another tool is the direct minting/burning of DAI through the DAI/USDC Peg Stability Module, which defends the 1:1 peg. This mechanism allows large-scale DAI issuance or redemption to counteract excessive market volatility.

- An Emergency Shutdown could be triggered as a last resort if the system faces severe instability, global settling DAI collateral and returning underlying assets. However, no Emergency Shutdown has occurred since DAI's launch.

On reserve management and transparency, we observed that:

- DAI reserves are collectively managed by the MakerDAO decentralized autonomous organization (DAO) through on-chain governance processes. Members signal approval/disapproval for reserve changes through transparent voting mechanisms.
- All proposals and changes to DAI's collateral framework and parameters are documented on-chain and publicly accessible. This includes adjustments to risk parameters, new collateral onboarding, changes to the DSR, etc.
- Major protocol alterations require Multi-Collateral DAI (MCD) system spells to enact technical changes after governance approval. Spells are executable code that modifies system parameters according to passed governance votes.
- Third-party audits provide independent assessments of DAI's smart contract codebase. Ongoing audits and formal verification offer additional transparency into DAI's technical integrity.
- Public block explorers allow real-time monitoring of DAI collateral composition, supply metrics, governance activity, and other on-chain data.

crvUSD has emerged as a pioneering stablecoin conceived by Curve Finance, embodying an innovati methodology in the domain of protocol risk containment. The issuance and redemption processes of this stablecoin are intricately orchestrated through dual operational frameworks:

- Over-collateralized Collateralized Debt Position (CDP) system where each crvUSD is backed by collateral and secured by AMM bi-directional conversion mechanism - LLAMMA.
- Algorithmic-based peg-keeping system that consists of 3 peg mechanisms: LLAMMA invariant (oracle combination), Stabilizer (PegKeepers) and Borrow rate Monetary Policy

The Curve CDP protocol is ingeniously crafted to transcend conventional DeFi liquidation paradigms, introducing an AMM bi-directional conversion methodology, encapsulated in the LLAMMA module. This innovation is instrumental when collateral value diminishes, initiating a 'soft liquidation' sequence that liquidates the collateral in exchange for crvUSD. Conversely, an augmentation in collateral value triggers a repurchase mechanism, restoring the user's position.

The LLAMA pool is structured around two core components – the collateral asset and "Bands," which delineate distinct price ranges of the collateral. When initiating a CDP position, users engage with the crvUSD Controller and are required to specify several parameters.

The Controller serves as the administrator for the crvUSD module. It processes inputs from various sources to ensure the effective operation of the protocol. These inputs come from stablecoin users, including the amount of collateral provided, the borrowed stablecoin amount, and the number of bands, among other loan management functions.

Parameters subject to the user's specification include the amount of collateral to be deposited, the quantity of crvUSD to be borrowed, and the Band range that will encompass the deposited collateral. It is imperative for users to contribute liquidity to a minimum of five bands, with the upper limit capped at fifty bands. Each band is instrumental in defining specific collateral price echelons, streamlining the process of collateral management and risk mitigation.

LLAMMA's finesse extends to enhanced user position management, facilitated by the division of collateral into distinct band ranges. Every band is characterized by its distinct upper and lower price limits, interconnected by a cross-point that bridges consecutive bands. This design ensures a seamless transition, where the apex of one band seamlessly aligns with the base of the subsequent one. 'Soft liquidations' are executed within a designated 'active band,' a feature that ensures liquidations are compartmentalized and controlled. When a user's position descends beneath this active band, the system is configured to facilitate only crvUSD debt repayment, prohibiting collateral augmentation as a means of position defense. In contrast, an ascending collateral price activates a counter mechanism, instigating a de-liquidation process where crvUSD is systematically exchanged back into the original collateral. This dual-action mechanism underscores the crvUSD system's adaptive nature, bolstering its resilience and ensuring sustained equilibrium amidst market volatility.

Proper crypto-backed stablecoins are fully collateralized by digital assets that exist outside the stablecoin arrangement and are otherwise unaffiliated with the promoter of the stablecoin. Well-designed crypto-asset-collateralized stablecoins have established strong track records of resilience through periods of market stress, unlike uncollateralized stablecoins that are susceptible to volatility in value.

Below we offer comprehensive comments pertaining to the specific stipulations enumerated under Article 7 of RTS. By addressing each point sequentially, we aim to ensure clarity, precision, and a thorough exploration of the nuances associated with every provision.

Article 7
Liquidity management, reserve assets, and redemption rights
1. The application shall contain the following information ensuring compliance with the requirements on liquidity management and on the reserve assets:

(i) the comprehensive and detailed framework illustrating the constitution, composition, management, and segregation of the reserve of assets, in accordance with the requirements set out in Article 36 of Regulation (EU) 2023/1114, and in the EBA RTS on reserve of assets. Where the applicant applies for voluntary classification of asset-referenced tokens as significant asset-referenced tokens, the framework shall contain the liquidity management policy and procedures. The framework shall also illustrate the reporting lines to the management body and how the management body's responsibility for the prudent management of the reserve of assets will be ensured;

We suggest recognition of the whitepaper descriptions for the purpose of an in-depth overview of reserve setup and management. The meaning of the term "whitepaper"

coincides with the provision of Recital 24 MiCAR: *information document containing mandatory disclosures ('a crypto-asset white paper').*

The composition of asset reserves is typically detailed in the crypto asset's whitepaper. This document serves as an initial blueprint and offers potential stakeholders a comprehensive overview of the project's intentions, structural underpinnings, and guiding principles. Moreover, it is pertinent to understand that decentralized projects, especially those governed by Decentralized Autonomous Organizations (DAOs), champion decentralized decision-making processes. Consequently, the ongoing management, allocation, and segregation of assets are typically entrusted to the collective will of the DAO members.

In terms of procedure, voting is the cornerstone of decision-making within a DAO. Votes can be conducted either on-chain, utilizing blockchain's transparent and immutable attributes, or off-chain, depending on the stipulations agreed upon by the community. These votes, the outcome of which is not predetermined, can touch upon a myriad of aspects, including but not limited to, adjustments to reserve parameters or the potential reallocation of assets.

Example of DAO decision-making process:

https://messari.io/governor/proposal/552430e8-2c1b-4b29-907b-1f959a757097
https://messari.io/governor/proposal/90f89287-b495-434e-b510-3924872e8d1f
https://gov.curve.fi/t/proposal-to-add-stbt-3crv-to-the-curve-gauge-controller/9013

(ii) the clear and detailed policy describing the stabilisation mechanism of the asset-referenced token for which the authorisation is sought;

The project whitepaper, along with the constantly updated supporting documentation, offers a meticulous and in-depth elucidation of the stabilization mechanism's logic, setup, and execution. We are of the opinion that the mentioned paperwork substantially describes the mechanisms powering the asset-referenced token stability.

Herewith we provide a relevant example with the Curve approach to token stabilization through CDP on the LLAMMA algorithm. This collateral is incorporated into LLAMMA within specific price parameters. If the collateral's price decreases gradually, the collateral is transformed into an adequate amount of crvUSD, ensuring the CDP is maintained. This transformation can be facilitated through self-liquidation or external intervention if the coverage nears risky boundaries or is safely distant, hoping for a price rebound.

Upon depositing collateral and taking out stablecoins, the LLAMMA algorithm determines the price bands for positioning the collateral. Should the collateral's price fluctuate, it begins conversion to stablecoin. When the system is "underwater", borrowers have sufficient funds to offset their loan. If this function indicates values nearing liquidation limits, an external entity may step in to handle the liquidation. Typically, this isn't immediate and might take days or weeks after the collateral price has decreased and stabilized. It might not even be necessary if the collateral price rebounds promptly.

The chief instrument to sustain the parity of crvUSD with the USD is encapsulated within the "PegKeeper" algorithm. This computational protocol dynamically modulates both the applicable interest rate and the predetermined liquidation ratio contingent upon the prevailing supply and demand factors affecting crvUSD. Such modulations are meticulously calibrated to harmonize the issuance and requisition of crvUSD, thereby safeguarding that its market value remains collateralized.

PegKeeper contract serves as mechanism control for crvUSD stable-pool:

- If crvUSD increases above 1$ (ps > 1) Curve v1 pool is in imbalance and PegKeeper mints uncollateralized crvUSD into stable-pool to increase crvUSD pool supply. Uncollateralized crvUSD can only be minted (deposited) into Curve v1 pools as single-side liquidity and will be recorded as PegKeeper debt.
- If crvUSD decreases below 1$, PegKeeper will start withdrawing previously minted crvUSD from the stable pool and burn it to reduce crvUSD pool supply. PegKeepers in that way repay the debt of minted uncollateralized cvrUSD.

The rate of borrowing within the framework is inherently fluid, and meticulously calibrated to mirror the prevailing dynamics of the asset pool. Instances where the collateral's value experiences a decline, propelling certain positions into a phase of mild liquidation, can precipitate a reduction in the borrowing rate. This diminished rate acts as a catalyst, encouraging users to initiate borrowing and facilitate the disposal of assets. Conversely, an augmentation in the rate serves as a stimulus for users to acquire crvUSD and satisfy their outstanding debts.

In the event that primary corrective measures prove insufficient in maintaining the crvUSD's parity with the dollar, the final line of defense, i.e. Monetary Policy is activated. This policy is characterized by the implementation of a formula designed to exponentially escalate the borrow rate of crvUSD, inducing an upward trajectory in price indices across various bands. Such a tactical maneuver is intended to incentivize borrowers to expedite the settlement of their crvUSD liabilities, circumventing the escalation of their positions into the active band, thereby reinforcing the stability and integrity of the financial ecosystem.

(iii)the name of the external consultant who will be in charge of the independent audit on the reserve of assets every six months in accordance with Article 36, paragraph (9) of Regulation (EU) 2023/1114;

The reserve of assets maintained in liquidity pools cannot be assessed and verified in a conventional way. Therefore our suggestion is to expand the recognition to third-party audits regularly carried out over protocol smart contracts. DAOs commanding protocol governance employ a strategy to maximize security by combining formal verification efforts with more traditional security audits paired with higher-level formal modeling. A common approach is to have several leading independent security auditors to protect against logical errors and/or potential failure modes in the contract logic aided by bug bounty programs.

(iv)the detailed policy and procedures on the custody of the reserve assets, including the selected custody modality, ensuring compliance with the requirements set out in Article 37 of Regulation (EU) 2023/1114;

(v) the clear and detailed investment policy of the reserve assets in accordance with the requirements set out in Article 38 of Regulation (EU) 2023/1114 and with EBA RTS on the financial instruments that can be considered highly liquid and bearing minimal market risk, credit risk and concentration risk in accordance with Article 38(5) of Regulation (EU) 2023/1114;

(vi)the details of the contractual arrangements entered into with third-parties for the operation, the investment and the custody of the reserve assets, in accordance with the policies referred to in points (iv) and (v).

We respect the necessity to draw up a clear framework for reserve custody in conjunction with Article 37 of Regulation (EU) 2023/1114. At the same time, we share the view that DAO interconnectedness has a positive influence on the policies elaboration, reflecting the views of all stakeholders. Putting an investment proposal to a community vote is the best example of a transparent process during which voters can signal their support or opposition to the proposed allocation. Such voting takes place after certain preparation, detailed studies, and opinions from competent external consultants. All mentioned documentation shall be disclosed to the community to ensure an informed decision is made. Financial, technical and legal assessment is conducted to inform governing members' position before voting. The subject of their decision may also be specific parameters of the agreement, e.g. term and type of storage, disposal of the funds and others. Therefore, there are no technical obstacles to implementing specific requirements and/or restrictions regarding the type of financial instruments in which the reserves will be invested.

A DAO proposal serves as a concrete suggestion presented by a member or the larger community for the DAO's deliberation. This document elucidates the concept, its execution strategy, and the financial resources required for its fruition. Ideally, proposals should be well-thought-out suggestions that have progressed beyond mere musings and are poised for community scrutiny.

Given the detailed nature of DAO proposals and the comprehensive evaluation process they undergo, our suggestion is to consider the DAO proposal submission and approval procedure to be recognized as a legitimate method to document the custodial and investment responsibilities of an ART issuer under Chapter 3 of Regulation (EU) 2023/1114. If a proposal meets the qualifying benchmarks for voting initiation and subsequently secures a favorable community vote, it stands to reason that all requisite policies, procedures, and contractual arrangements are aptly documented. Novel voting mechanisms within DAOs not only capture the minutest asset portfolio adjustments but also facilitate instantaneous implementation of risk mitigation measures, having received endorsement from the governing entity.

Examples:

https://vote.makerdao.com/polling/QmdRELY7#poll-detail

https://vote.makerdao.com/polling/Qmf3y9vG#vote-breakdown
https://governance.aave.com/t/temp-check-aave-treasury-proposal-for-rwa-allocation/14381

In the discourse on DAO governance, elucidating its intricate safeguards, we have to highlight the exemplary role of veCRV mechanics. This model showcases advanced preventative measures designed to thwart potential governance attacks, embodying a synthesis of innovation and security.

veCRV stands for vote-escrowed CRV, it is non-transferable and can be locked for a period of 1 to 4 years at 0.25 to 1 conversion rate. The longer one locks CRV, the more veCRV they receive. While promoting long-term engagement and stability, this construct enhances security by requesting tokens to be locked for voting. Vote locking leads to the temporary removal of CRV tokens from the circulating supply, instigating a reduction in available tokens. This lowers supply driving up price and market cap. Furthermore, veCRV, characterized by its non-transferable nature, ensures that individuals who have engaged in vote locking are firmly anchored to their positions throughout the lock's tenure, fostering a committed and stable governance environment.

The voting power decreases linearly over time, ensuring that active participation is required to maintain influence. veCRV holders receive boosts on their provided liquidity, incentivizing more users to participate in governance. With more participants, the governance becomes more decentralized, reducing the risk of malicious attacks or undue influence.

In summary, veCRV enhances governance security by ensuring that participants are committed and engaged, promoting decentralization, and implementing checks and balances through mechanisms like voting power decay.