

ARSX Engine Smart Contract Audit Report (Extended)





Overview

This updated audit analyzes the ARSX Engine smart contract, taking into account previous audits, the introduction of a self-managed custom oracle, and the potential addition of a Peg Stability Module (PSM).

Summary

- **Contract Name:** ARSXEngine
- **Author:** Rodrigo Garcia Kosinski
- **Reviewed Features:** Collateral management, minting/burning, stability mechanisms, oracle integration, possible PSM integration

Security Analysis

-  Proper access control using `Ownable`
-  Strict collateral ratio checks and validations
-  Reverts on invalid collateral or price issues
-  New custom oracle reduces external dependency but requires careful off-chain update governance

Gas Efficiency

- Efficient storage usage
- Clean error handling and minimal state changes
- Oracle now simplified with direct push model (no request callbacks), reducing gas

Code Quality & Best Practices




- Clear separation of logic
- Custom errors to save gas
- Detailed revert messages and thorough edge case checks

Oracle Changes

The new self-managed oracle is a manual, push-based design. This removes Chainlink Functions' operational costs and complexities, but introduces: - Need for strong off-chain security (e.g., multisig, off-chain cronjobs) - Careful timestamp-based staleness validation

Peg Stability Module (PSM) Consideration

To further strengthen ARSX peg robustness, a PSM module similar to DAI's can be introduced. The PSM allows direct minting and redemption against stablecoins (e.g., USDC) at a fixed rate with minimal fees.

This provides: -  Improved liquidity and peg stability -  Additional arbitrage opportunities to keep ARSX stable -  Enhanced user confidence during market shocks

Risks of PSM

- Exposure to centralized stablecoin risks (e.g., USDC freezes)
- Reserve depletion risk during massive redemptions
- Requires governance and monitoring

Recommendations

- Consider implementing the PSM module as an optional add-on with carefully configured fees.
- Establish strong off-chain governance procedures for oracle price updates.
- Add continuous monitoring of collateral ratios and oracle update timestamps.
- Regularly simulate attack scenarios (e.g., rapid price drops, large redemptions).

Conclusion

The ARSXEngine contract remains robust with proper on-chain checks. The new custom oracle simplifies on-chain operations but demands off-chain diligence. Adding a PSM module can significantly strengthen peg reliability.

Audit Prepared By: GPT-4o — July 2025