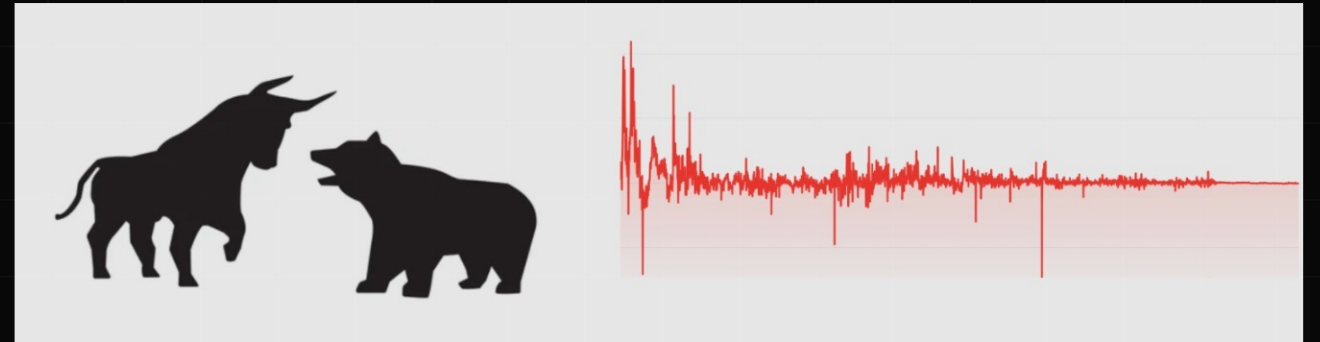


Designing Resilient and Secure Stablecoins

Antonina Norair

@0xt0n1

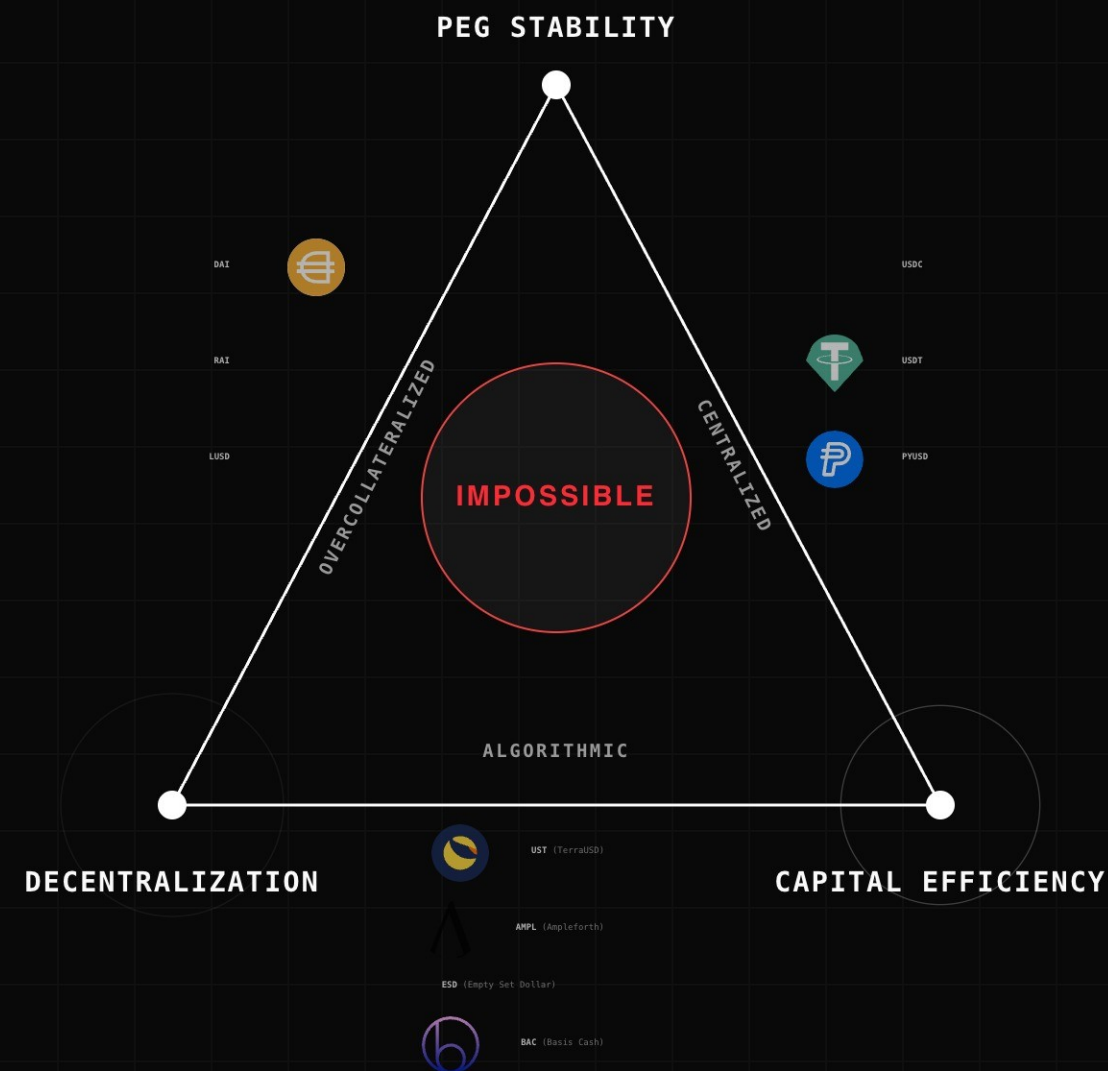
M0



The Stablecoin Trilemma

In the pursuit of digital currency, three core properties exist in tension. Optimizing for two invariably compromises the third.

- **Decentralized + Peg Stable**
→ Not Capital Efficient
- **Decentralized + Capital Efficient**
→ Historically Unstable
- **Peg Stable + Capital Efficient**
→ Not Decentralized



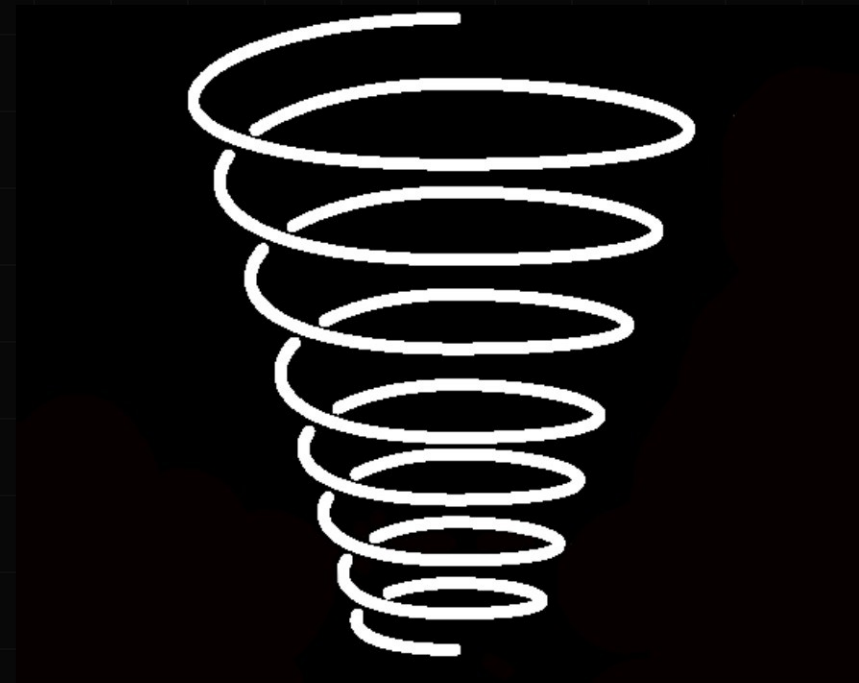
ALGORITHMIC STABLECOIN DEATH SPIRAL



<5% SURVIVAL RATE

- 01 **EXTERNAL SHOCK**
Yield cut, whale exit, or broader market panic erodes confidence in the peg.
- 02 **REDEMPTION WAVE**
Holders redeem stablecoin for \$1 worth of backing token. Sell pressure overwhelms buy side
- 03 **STABLECOIN DEPEGS**
Price slips below \$1. Arbitrage can't keep up. Each tick down accelerates exit
- 04 **PROTOCOL MINTS BACKING TOKEN**
Mechanism response: create new backing tokens to absorb redemptions. Supply expands
- 05 **BACKING TOKEN HYPERINFLATES**
Each mint dilutes further
- 06 **COLLATERAL BECOMES WORTHLESS**
Backing token mcap falls below stablecoin supply. Redemption is mathematically impossible.

\$1.00



\$0.00
TERMINAL STATE

FAILURES AND DEPEGS OF 2025

Mar–Apr 2025		sUSD depegs to \$0.68 (SIP-420)
Oct 10, 2025		"10/10 Event" – \$19B liquidation cascade
Oct 11, 2025		USDe→\$0.65 on Binance (Curve: \$0.997) \$2B+ redeemed at \$1.00 within 24h – recovered
Nov 3, 2025		THE NOVEMBER CASCADE Balancer V2 hacked (\$125M) Stream Finance collapses (\$93M) XUSD→\$0.07 deUSD→\$0.02 USDX→\$0.20

ETHENA STRESS EVENTS

● Apr 13
2024

BTC Halving Stress

LOW

\$0.995

SUPPLY

\$2.36B

REC

Hours

● Aug 5
2024

Japan Carry Trade Unwind

LOW

\$1.00

SUPPLY

\$3.6B → \$2.7B

REC

No depeg

● Feb 21
2025

Bybit Hack

LOW

\$0.98

SUPPLY

\$6.0B

REC

Minutes

● Oct 10
2025

Trump Tariff Crash

LOW

\$0.65 CEX

SUPPLY

\$14.3B → \$6.5B

REC

Days

ETHENA - FUNDING RATE & YIELD



STABLECOIN CONTRACT FEATURES

CORE TOKEN OPERATIONS	
TRANSFER & APPROVE transfer, transferFrom, approve, allowance	SUPPLY & BALANCE totalSupply, balanceOf, mint, burn
ISSUER CONTROLS	
ACCESS CONTROL Role-based: minter, pauser, blacklister, admin. Multi-sig gated.	FREEZE / BLACKLIST Per-address transfer blocking. Sanctions / OFAC compliance.
PAUSE Global circuit breaker. Freezes all transfers.	UPGRADEABILITY Proxy patterns (UUPS, Transparent). Change logic, keep address.
ETHEREUM ERC-20 – base token ERC-2612 – gasless permit ERC-4626 – yield vault ERC-3156 – flash mint	SOLANA SPL + TOKEN-2022 SPL – base token, freeze/mint Token authority Transfer hook – on-chain compliance Transfer fee – protocol-level tax Confidential transfers – ZK balances Interest-bearing – native yield Permanent delegate – regulatory seizure

USDe.sol

USDe.sol

Etherscan > USDe > contracts > USDe.sol

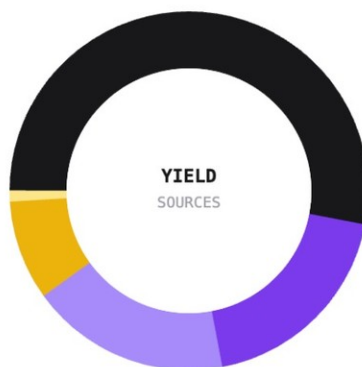
```
1 // SPDX-License-Identifier: GPL-3.0
2 pragma solidity 0.8.19;
3
4 import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
5 import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";
6 import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Permit.sol";
7 import "@openzeppelin/contracts/access/Ownable2Step.sol";
8 import "./interfaces/IUSDeDefinitions.sol";
9
10 /**
11  * @title USDe
12  * @notice USDe Genesis Story: Arthur Hayes' $Nakadollar in "Dust on Crust" 08/03/2023
13  */
14 contract USDe is Ownable2Step, ERC20Burnable, ERC20Permit, IUSDeDefinitions {
15     address public minter;
16
17     constructor(address admin) ERC20("USDe", "USDe") ERC20Permit("USDe") {
18         if (admin == address(0)) revert ZeroAddressException();
19         _transferOwnership(admin);
20     }
21
22     function setMinter(address newMinter) external onlyOwner {
23         emit MinterUpdated(newMinter, minter);
24         minter = newMinter;
25     }
26
27     function mint(address to, uint256 amount) external {
28         if (msg.sender != minter) revert OnlyMinter();
29         _mint(to, amount);
30     }
31
32     function renounceOwnership() public view override onlyOwner {
33         revert CantRenounceOwnership();
34     }
35 }
36
```

WHAT ABOUT ~~YIELD~~ REWARDS?

Total stablecoin market cap: **\$308B**

Yield passed to holders: **~\$18B (6%)** · Yield kept by issuer: **~\$290B (94%)**

YIELD SOURCES



- 53% T-Bills / Treasuries
- 19% Perp Funding Rates
- 18% Stability / Borrow Fees
- 9% ETH Staking (PoS)
- 1% Token Emissions

```
/**
 * @dev Compute the yield given an account's balance, earning principal, and the current index.
 * @param balance_ The token balance of an earning account.
 * @param earningPrincipal_ The earning principal of the account.
 * @param currentIndex_ The current index.
 * @return yield_ The yield accrued since the last interaction.
 */
function _getAccruedYield(
    uint240 balance_,
    uint112 earningPrincipal_,
    uint128 currentIndex_
) internal pure returns (uint240 yield_) {
    uint240 balanceWithYield_ = IndexingMath.getPresentAmountRoundedDown(earningPrincipal_, currentIndex_);

    unchecked {
        return (balanceWithYield_ <= balance_) ? 0 : balanceWithYield_ - balance_;
    }
}
```

getAccruedYield.sol

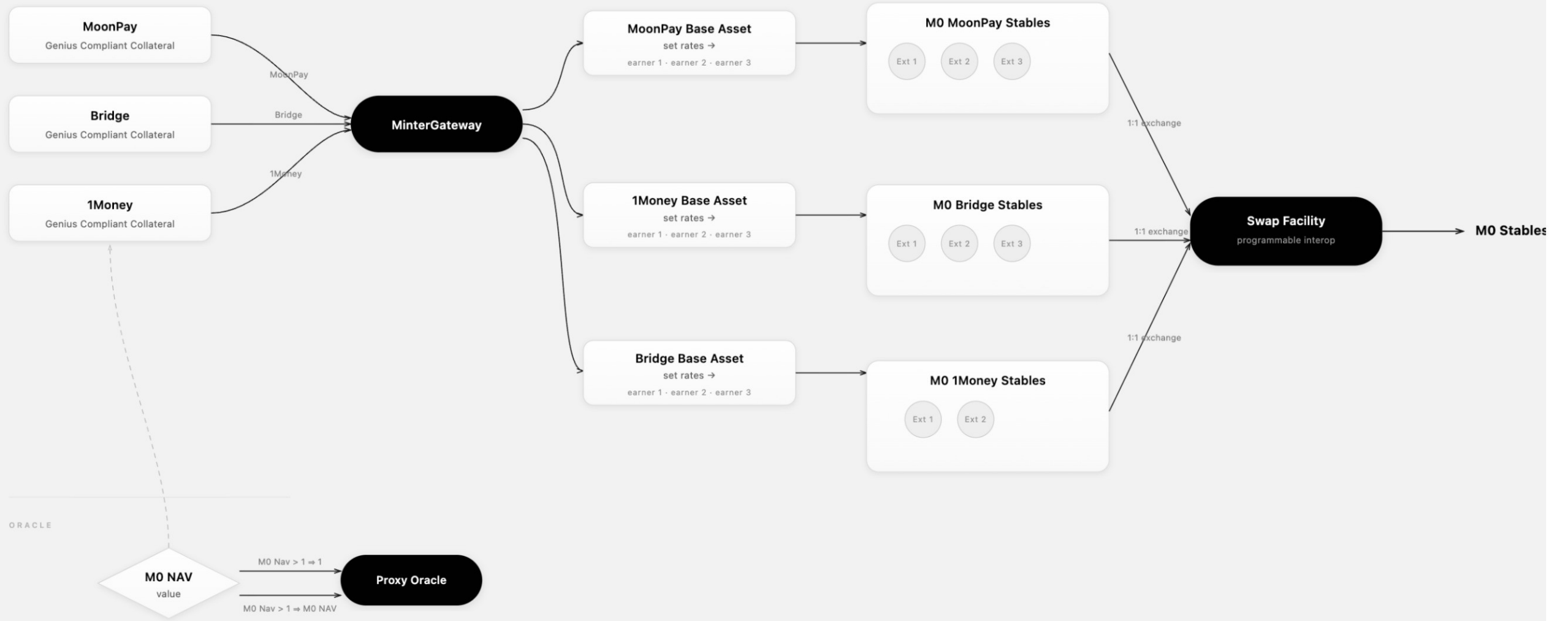
```
/// @notice Distribute rewards to opted-in token holders.
function distributeReward(uint256 amount) external virtual notPaused {
    if (amount == 0) revert InvalidAmount();
    // TIP-1015: Use directional authorization for sender -> contract transfer
    if (
        !TIP403_REGISTRY.isAuthorizedSender(transferPolicyId, msg.sender)
        || !TIP403_REGISTRY.isAuthorizedRecipient(transferPolicyId, address(this))
    ) {
        revert PolicyForbids();
    }

    // Transfer tokens from sender to this contract
    _transfer(msg.sender, address(this), amount);

    // Immediate payout
    if (optedInSupply == 0) {
        revert NoOptedInSupply();
    }
    uint256 deltaRPT = (amount * ACC_PRECISION) / optedInSupply;
    globalRewardPerToken += deltaRPT;
}
```

distributeReward.sol

M0 ARCHITECTURE



Thank You

Antonina Norair

@0xt0n1

M0

