CHAOS LABS

USDV Risk and Economic Security Assessment

A rigorous analysis of USDV, a stablecoin backed by STBT, detailing mechanisms, associated risk vectors, and featuring recommendations for risk mitigation and secure asset onboarding.

Verified USD Foundation

November 9th, 2023

USDV Risk and Economic Security Assessment

Omer Goldberg
omer@chaoslabs.xyz

Shai Kritz
shai@chaoslabs.xyz

November 2023

Abstract

Between November 1st and November 14th, 2023, Chaos Labs undertook a rigorous risk assessment for the USDV Foundation to evaluate the USDV stablecoin's architecture and operational dynamics. Throughout this engagement, our team conducted a holistic review of USDV's end-to-end mechanism, including its interactions with ecosystem actors and dependencies, to discover and quantify any exposures to outsized risk vulnerabilities. This encompassed a thorough analysis of potential design issues and a rigorous evaluation of the stablecoin's security posture to identify inherent weaknesses.

This risk assessment examines the inherent complexities of USDV's operations, including its unique tokenomics, the integration of ColorTrace for on-chain attribution, and its initial reliance on STBT as a backing asset. We begin with an in-depth examination of USDV's stablecoin mechanism design, scrutinizing its structural integrity and resilience against market volatility. We delve into the nature and quality of the backing assets, assessing their capacity to underpin the stablecoin's value. A focal point of our review is using tokenized Treasury Bills and Reverse Repurchase Agreements as a backing strategy, where we analyze the implications for liquidity and stability.

Furthermore, we navigate the complex legal and regulatory framework surrounding USDV, identifying potential challenges and compliance considerations that could impact its operability across jurisdictions. The assessment addresses liquidity and oracle risk, evaluating the robustness of the mechanisms in place to mitigate the risks associated with price information sources and liquidity provisions.

We dissect the USDV rebasing mechanism to better understand its potential influence on the stablecoin's stability, especially in response to market pressures that could lead to depegging events. We thoroughly explore depeg risk, considering historical precedents and current market dynamics. Counterparty risk is another critical aspect of our analysis, where we assess the implications of USDV's interactions with various stakeholders in the DeFi ecosystem.

In evaluating the ColorTrace algorithms, we also investigate potential attack vectors that malicious ecosystem actors could exploit to maximize unearned yield shares. This analysis is critical for understanding the algorithm's security posture and recommending measures to mitigate such exploitative tactics.

This assessment aims to aid potential integration and partner protocols in onboarding the USDV asset. It is designed to provide a deep understanding of the operational and on-chain mechanisms powering USDV, offering a comprehensive view of the risk surface. As this is a pre-launch assessment, it's crucial to note that the absence of live market data constrains our insights on market and liquidity risks. Therefore, we strongly recommend continuous monitoring post-launch and suggest a renewed assessment as USDV grows and matures.

The conclusion of this assessment summarizes our findings. It provides strategic recommendations tailored to establish USDV's market position, enhance its risk resilience, and optimize its operational framework for long-term stability and investor confidence. Through this assessment, Chaos Labs aims to deliver actionable insights that will guide USDV's stakeholders in navigating the complex and evolving terrain of DeFi risk.

Contents

Disclaimer

This document is purely informational and does not constitute an invitation to acquire any security, an appeal for any purchase or sale, or an endorsement of any financial instrument. Neither is it an assertion of the provision of investment consultancy or other services by Chaos Labs Inc. References to specific securities should not be perceived as recommendations for any transaction, including buying, selling, or retaining any such securities. Nothing herein should be regarded as a solicitation or offer to negotiate any security, future, option, or other financial instrument or to extend any investment advice or service to any entity in any jurisdiction. The contents of this document should not be interpreted as offering investment advice or presenting any opinion on the viability of any security, and any advice to purchase, dispose of or maintain any security in this report should not be acted upon. The information contained in this document should not form the basis for making investment decisions.

While preparing the information presented in this report, we have not considered individual investors' specific investment requirements, objectives, and financial situations. This information does not account for the specific investment goals, financial status, and individual requirements of the recipient of this information, and the investments discussed may not be suitable for all investors. Any views presented in this report by us were prepared based on the information available when these views were written. Additional or modified information could cause these views to change. All information is subject to possible rectification. Information may rapidly become unreliable for various reasons, including market or economic changes.

Chapter 1

Overview

1 USDV Overview

The stablecoin ecosystem has been a cornerstone of the DeFi space, with significant issuers like Circle and Tether at the helm, catalyzing growth through their issuance of digital currencies backed by real-world assets such as U.S. government Treasury bills, gold, and cash reserves. Their business model is elegantly simple yet effective: they generate a yield from the assets backing the stablecoins and collect transaction fees from applications that drive demand for these currencies. These companies have adeptly managed the supply side of stablecoins, creating a reliable and scalable digital currency source that mirrors the stability of traditional fiat currencies.

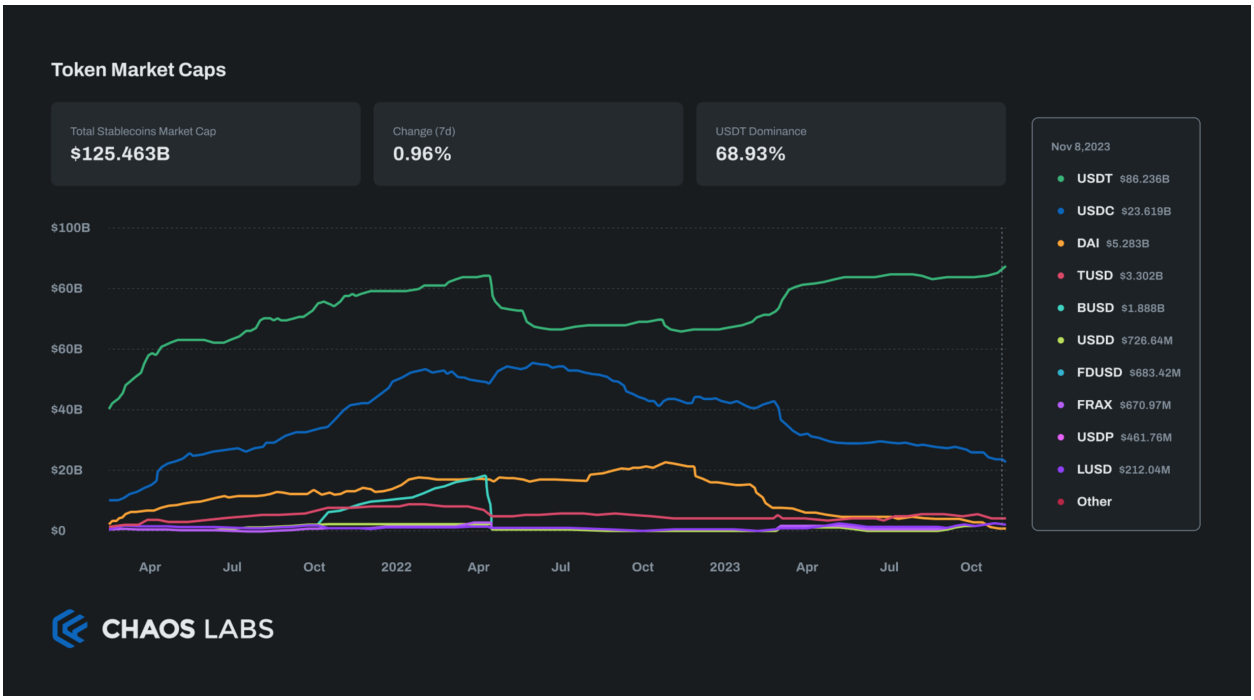
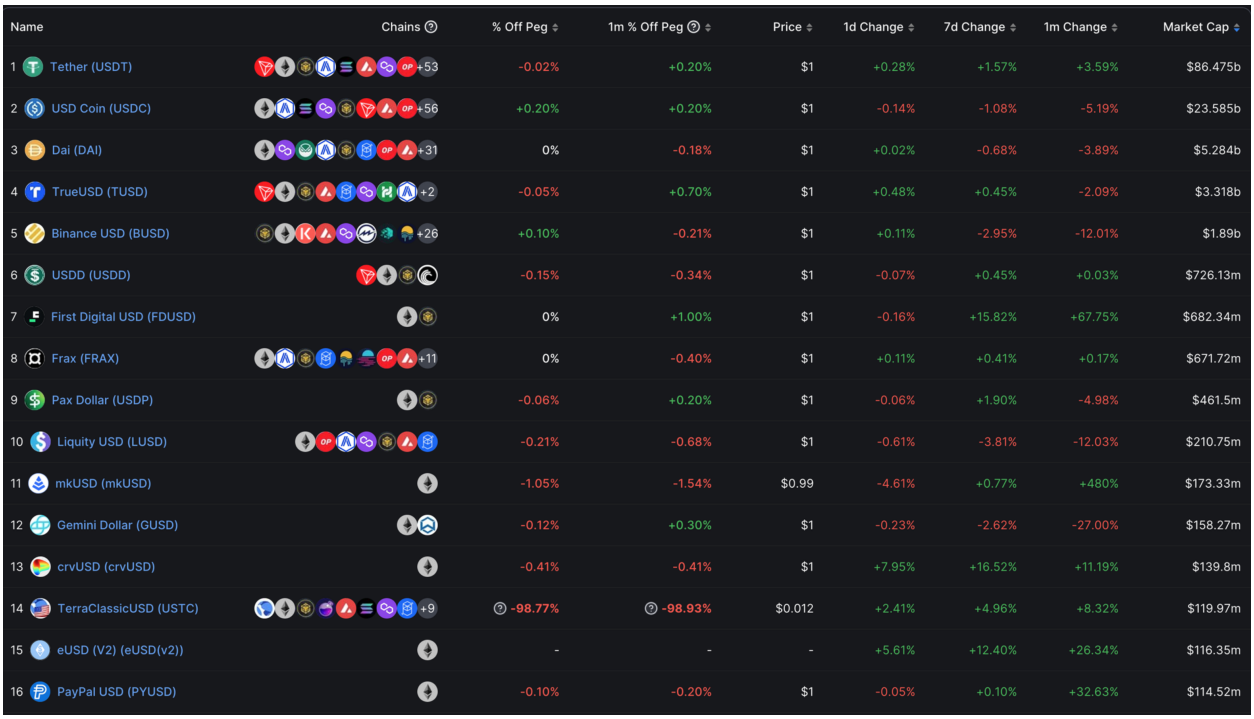


Figure 1.1

However, a critical imbalance exists within this model. Applications that generate stablecoin demand—vital in the DeFi machine—have been excluded from participating in the yield

generated by the assets backing stablecoins. This issue stems from a longstanding challenge: the computational and storage demands of tracking every stablecoin transaction have been prohibitively expensive and complex, making it unfeasible to create a more equitable system where demand-generating applications can benefit from the yields. Enter USDV, a novel stablecoin that recognizes this gap and presents a novel solution. USDV is engineered to solve current stablecoin limitations by offering features that enhance user experience, scalability, and financial security. At its core, USDV addresses the Fungible Token Coloring Problem, which has hindered stablecoin issuers' ability to track and reward entities that generate token demand by implementing ColorTrace, an algorithm developed by LayerZero Labs.



Name	Chains	% Off Peg	1m % Off Peg	Price	1d Change	7d Change	1m Change	Market Cap
1 Tether (USDT)	+53	-0.02%	+0.20%	$1	+0.28%	+1.57%	+3.59%	$86.475b
2 USD Coin (USDC)	+56	+0.20%	+0.20%	$1	-0.14%	-1.08%	-5.19%	$23.585b
3 Dai (DAI)	+31	0%	-0.18%	$1	+0.02%	-0.68%	-3.89%	$5.284b
4 TrueUSD (TUSD)	+2	-0.05%	+0.70%	$1	+0.48%	+0.45%	-2.09%	$3.318b
5 Binance USD (BUSD)	+26	+0.10%	-0.21%	$1	+0.11%	-2.95%	-12.01%	$1.89b
6 USDD (USDD)		-0.15%	-0.34%	$1	-0.07%	+0.45%	+0.03%	$726.13m
7 First Digital USD (FDUSD)		0%	+1.00%	$1	-0.16%	+15.82%	+67.75%	$682.34m
8 Frax (FRAX)	+11	0%	-0.40%	$1	+0.11%	+0.41%	+0.17%	$671.72m
9 Pax Dollar (USDP)		-0.06%	+0.20%	$1	-0.06%	+1.90%	-4.98%	$461.5m
10 Liquity USD (LUSD)		-0.21%	-0.68%	$1	-0.61%	-3.81%	-12.03%	$210.75m
11 mkUSD (mkUSD)		-1.05%	-1.54%	$0.99	-4.61%	+0.77%	+480%	$173.33m
12 Gemini Dollar (GUSD)		-0.12%	+0.30%	$1	-0.23%	-2.62%	-27.00%	$158.27m
13 crvUSD (crvUSD)		-0.41%	-0.41%	$1	+7.95%	+16.52%	+11.19%	$139.8m
14 TerraClassicUSD (USTC)	+9	-98.77%	-98.93%	$0.012	+2.41%	+4.96%	+8.32%	$119.97m
15 eUSD (V2) (eUSD(v2))		-	-	-	+5.61%	+12.40%	+26.34%	$116.35m
16 PayPal USD (PYUSD)		-0.10%	-0.20%	$1	-0.05%	+0.10%	+32.63%	$114.52m

Figure 1.2

ColorTrace tackles on-chain token attribution by enabling 'token coloring' for all USDVs in circulation, allowing for the segmentation by Verified Minters based on unique Color IDs. This technology ensures complete traceability and fair yield distribution, promoting equitable reward distribution based on user demand and engagement. USDV is natively cross-chain, adopting the Omnichain Fungible Token (OFT) standard for maximum interoperability and scalability, enhancing security and liquidity. Underlying assets are securely stored in a globally unique Vault on the Ethereum blockchain, with the first reserve asset being the Short-term Treasury Bill Token (STBT)—a risk-free yield-bearing asset pegged 1:1 with the USD. In conclusion, USDV aims to be more than just a stablecoin; it seeks to be a transformative financial instrument offering a scalable, secure, and equitable platform for digital transactions, ensuring that all participants in the ecosystem are recognized and rewarded for their contributions, thus paving the way for a more inclusive stablecoin economy.

2 Audit Objectives

2.1 Assessment Goals

Chaos Labs' assessment is designed to review the structural resilience and economic security of the USDV stablecoin. Our audit is crafted to dissect the nuances of USDV's design and defensive mechanisms against a spectrum of financial adversities.

Our analysis provides a granular examination of the following pivotal domains:

- **Asset Backing Analysis**: We delve into the composition and robustness of the assets underpinning USDV. We scrutinize their liquidity and risk profiles to validate the stablecoin's foundation on low-risk and inherently stable assets.
- **Reward Mechanism Scrutiny**: The minter reward mechanism undergoes a rigorous evaluation to identify any potential for exploitation that could lead to disproportionate reward acquisition, which could undermine the equitable ethos of the system.
- **Depegging Risk Assessment**: The protocols and contingencies established to avert and manage depegging scenarios are evaluated to ascertain the steadfastness of USDV's capacity to maintain its peg across fluctuating market landscapes.
- **STBT Mechanism and Liquidity Analysis**: We dissect the operational mechanics of the STBT mechanism and its influence on the liquidity dynamics of USDV, seeking to establish its integral role within the stablecoin's economic architecture at launch.
- **Minter Deficit Contingency Evaluation**: The assessment contemplates the provisions and strategies for scenarios where a minter encounters a deficit, ensuring the system's architecture supports sustainable reminting processes.
- **Flash Loan Vulnerability Analysis**: Our scrutiny extends to the system's resilience against flash loan exploits, focusing on the potential for such maneuvers to unjustly skew the token coloring process, affecting distributors or TVL aggregators.

2.2 Scope Clarification and Constraints

In the spirit of academic rigor and precision, Chaos Labs delineates the boundaries of this assessment with clarity, identifying areas that fall outside the ambit of our current engagement:

2.3 Out of Scope - Smart Contract Code Examination

The intricate analysis of smart contract code and the minutiae of its operational implementation are outside the scope of this assessment. Below, we link to relevant smart contract security audits:

- USDV: Zellic Security Assessment
- USDV: Ottersec Security Assessment
- USDV: Paladin Security Assessment
- STBT Audits

Instant Finality Verification

This assessment does not extend to confirming transaction finality guarantees within the USDV framework.

Cross-Chain Messaging Evaluation

This review does not examine cross-chain messaging systems' robustness and security protocols.

Infrastructure Review

The extensive infrastructure undergirding the USDV project, including crucial custody solutions and market-making mechanisms, is outside the purview of this assessment.

Scope of Work Conclusion

Acknowledging the inherent limitations imposed by the temporal constraints of security assessments is imperative. As such, while the primary lens of our assessment is trained on the strategic conception and architectural blueprint of USDV, with a particular emphasis on its pioneering asynchronous cross-chain capabilities, the review of its practical implementation is approached with a secondary emphasis. Our investigative efforts are dedicated to unraveling the systemic design elements central to the economic security and risk profile of USDV.

Chapter 2

USDV Overview

1 Protocol Primer

The architecture of the USDV stablecoin protocol serves as the bedrock upon which our risk assessment is constructed. A thorough comprehension of the protocol's structure is paramount, as it informs the development of robust risk models that are both precise and contextually relevant. This section is dedicated to meticulously delineating the fundamental pillars of the end-to-end USDV protocol. By dissecting and understanding each component's function and interdependencies, we lay the groundwork for a nuanced evaluation of the protocol's risk landscape.

The USDV protocol is a complex combination of technological innovations and financial mechanisms, each serving a distinct purpose yet collectively contributing to the protocol's overarching objective of providing a stable, secure, equitable, and scalable digital currency. We must first establish a granular understanding of these components—from asset backing and minting processes to yield distribution and oracle integration—before we can accurately identify and model potential risks.

In the subsequent sections of this risk assessment, we will delve deeper into each of these foundational pillars. Our analysis will extend beyond mere functional descriptions to critically examine the risk surfaces they present. This will involve an exploration of the technical intricacies, economic mechanisms, and operational procedures that underpin the USDV protocol. By doing so, we aim to comprehensively enumerate the risks associated with each component and develop sophisticated models that can predict, quantify, and mitigate these risks effectively.

This introductory exploration is designed to inform and equip stakeholders with the necessary insights to navigate the complex interplay of factors that govern the USDV ecosystem. As we progress through the assessment, each section will build upon the last, culminating in a detailed and articulate exposition of USDV's risk architecture. This systematic approach ensures that our risk assessment is grounded in a deep and systematic understanding of the USDV protocol, ultimately enabling a strategic and informed risk management posture.

The USDV stablecoin enables tracking on-chain token demand attribution generated by applications, termed the *Fungible Token Coloring Problem*. Lack of token-flow tracking and proper attribution hinders the fair distribution of rewards by stablecoin issuers to entities that generate token demand. LayerZero's ColorTrace algorithm and solution also dictate the technical requirements and architecture, which we'll review below.

1.1 USDV Contract and Cross-Chain Functionality

The USDV contract, an ERC20 token, incorporates administrative features for compliance and utilizes signature-based permit interfaces on EVM chains. It manages local coloring states and synchronizes this information with the Ethereum Vault to minimize divergence. Deployed omnichain, USDV leverages LayerZero's messaging protocol and OFT standard for its immutable, permissionless, and censorship-resistant properties.

1.2 Token Flow and Attribution Technical Constraints and Solutions

Addressing this problem, USDV confronts two significant technical constraints:

1. Impracticality of maintaining per-minter attribution due to local storage limitations.
2. Complexities of cross-chain communication.

LayerZero's approach to the token coloring problem is pragmatic, requiring all transfers to recolor tokens to match the receiver's wallet balance, thereby simplifying the storage complexity to $O(1)$ for single-chain contexts. However, the challenge magnifies when considering the omnichain environment, where economic and safety constraints emerge due to crosschain messaging asynchrony.

1.3 Vault Mechanics and Delta Management

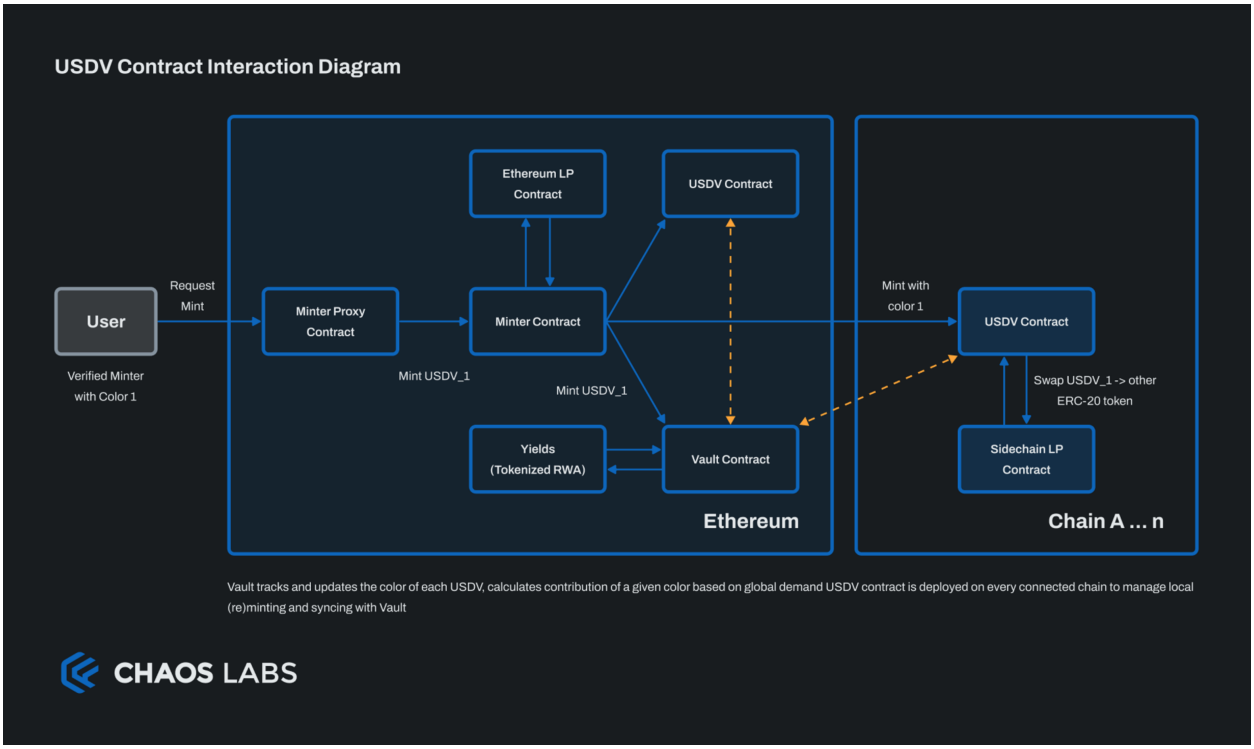


Figure 2.1

The USDV Vault, uniquely positioned on the Ethereum blockchain, is the source of truth of this mechanism. It is responsible for issuing, tracking, and updating the mint of each color,

which reflects the global circulation and demand for that color across all chains. This system enables the fair distribution of yields by the token foundation. To manage the divergence between mint and circulation, ColorTrace introduces the concept of $localMint$ and $delta$ Δ, which allows for an efficient and provably safe reconciliation of these values.

1.4 Minter Contracts and Coloring Dynamics

The USDV stablecoin employs a unique token coloring mechanism to track and attribute token demand generated by various entities within its ecosystem. This method involves tagging or overriding token metadata (Color ID) when USDV is 'touched' or 'converted'. Below, we delineate the distinct methods for coloring USDV tokens, each serving specific functions within the protocol.

Default Color

- **Definition**: Each Verified Minter is associated with a unique 'Default Color' color. This color represents a positive integer value in the token contracts and is unique to each Verified Minter.
- **Application**: Only Verified Minters can own and set Default Colors. They can assign these colors to contract addresses such as pools, pairs, wallets, and vaults. Each address can only have one color.
- **Operator Delegation**: Verified Minters may appoint Operators to set Default Colors on whitelisted addresses on their behalf.

1.5 Coloring Methods

Following the Default Color Rule

- **Mechanism**: If the receiver account sets a Default Color, all inbound tokens are recolored to match this.
- **Example**: If a pool with \$100 $USDV_{BLUE}$ receives \$120 $USDV_{RED}$ and has set BLUE as its Default Color, the inbound $USDV_{RED}$ is recolored to $USDV_{BLUE}$, resulting in a final balance of \$220 $USDV_{BLUE}$.

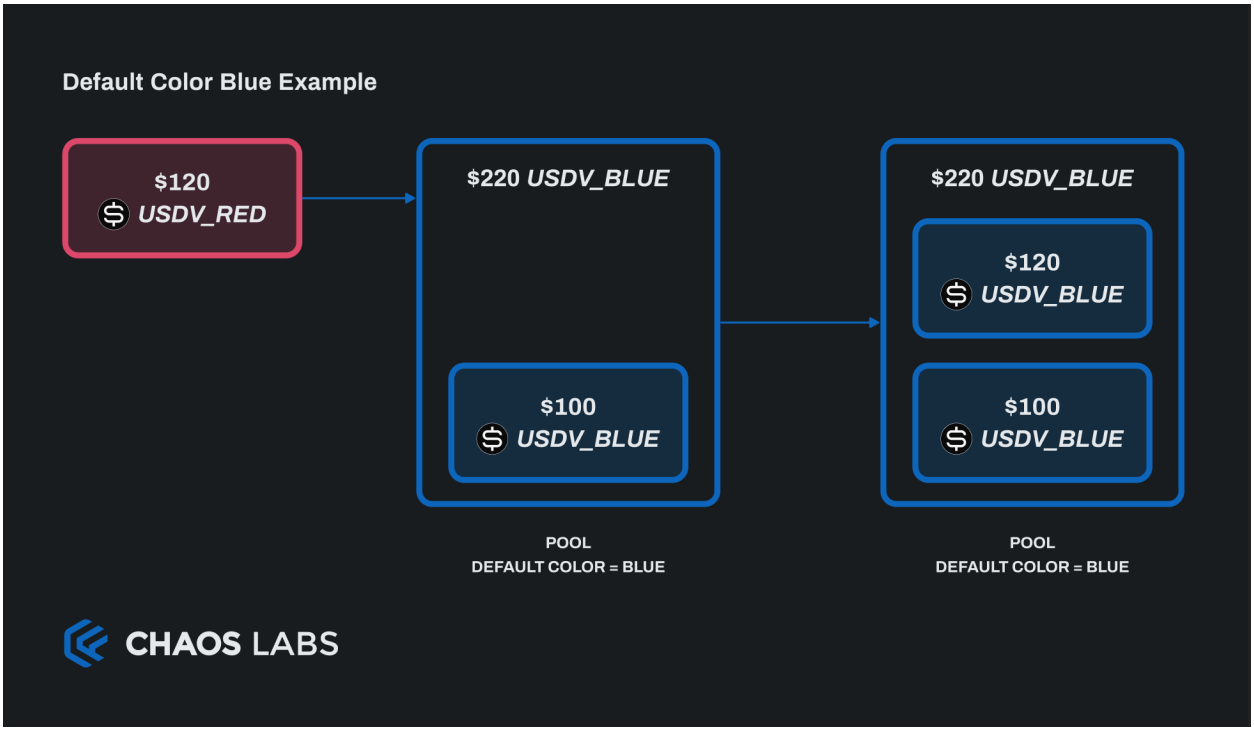


Figure 2.2

Coloring by Weight Rule

- **Mechanism**: In the absence of a set Default Color, the color with the larger balance is implicitly chosen as the Default Color for each transaction. The inbound tokens are recolored to match the color of the larger balance in the receiving account.
- **Example**: A pool with \$100 $USDV_{BLUE}$ receiving \$120 $USDV_{RED}$ would have the $USDV_{BLUE}$ recolored to $USDV_{RED}$ since \$120 > \$100, resulting in a final balance of \$220 $USDV_{RED}$.

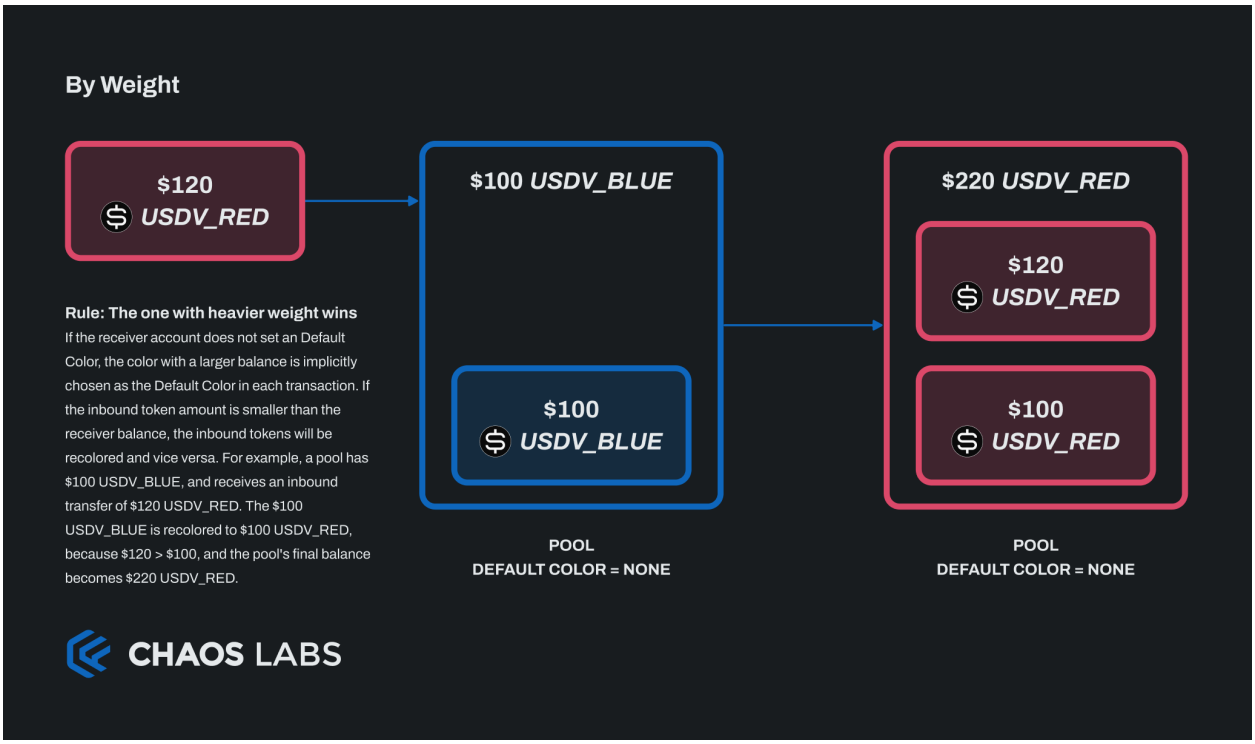


Figure 2.3

1.6 Additional Coloring Properties

- **Fungibility**: All tokens are fungible within a single address. This property allows for uniform incentivization of all inbound tokens in DeFi applications.
- **Longevity**: The color of tokens is long-lived. Tokens retain their designated color after withdrawal from DeFi Pools and maintain it until they undergo another recoloring process. This characteristic is vital in high-volume transaction protocols like decentralized exchanges (DeX), where users frequently deposit and withdraw tokens. The persistent color allows minters to accrue more attribution relative to their pools of Total Value Locked (TVL).

Each Verified Minter is assigned a unique color ID through a Minter contract, providing functionalities like blocklisting and alternative stablecoin minting configurations. The coloring process is KYC-gated, allowing eligible minters to obtain a color represented as a

positive integer within the token contracts. This process ensures that minted USDV carries the designated color, crucial for fair yield distribution.

1.7 Example: Interaction Between Two Minters

To illustrate the USDV coloring process in action, let's consider an example involving two distinct minters, each with its own designated color within the USDV ecosystem:

Scenario Setup

Minters: This scenario has two Verified Minters.

- Verified Minter 1: Associated with Color RED.
- Verified Minter 2: Associated with Color BLUE.

Initial Minting: Verified Minter 2 mints \$100 $USDV_{BLUE}$.

Coloring and Recoloring Process

- **Interaction with Pool**: The \$100 $USDV_{BLUE}$ minted by Verified Minter 2 enters a pool that has set its Default Color to RED.
- **Recoloring Action**: Upon interacting with this pool, the $USDV_{BLUE}$ tokens are recolored to align with the pool's Default Color. As a result, the \$100 $USDV_{BLUE}$ is transformed into \$100 $USDV_{RED}$.

Implications for Minters

- **Reminting by Verified Minter 1**: Following this recoloring event, Verified Minter 1 proceeds to remint all \$100 of the now $USDV_{RED}$, initially minted by Verified Minter 2.
- **Yield Share Advantage**: Verified Minter 1 gains control of the \$100 $USDV_{RED}$ due to this reminting action. This transfer of color and subsequent reminting action makes Verified Minter 1 eligible for a greater yield share, as they are now attributed with the minting of these recolored tokens.

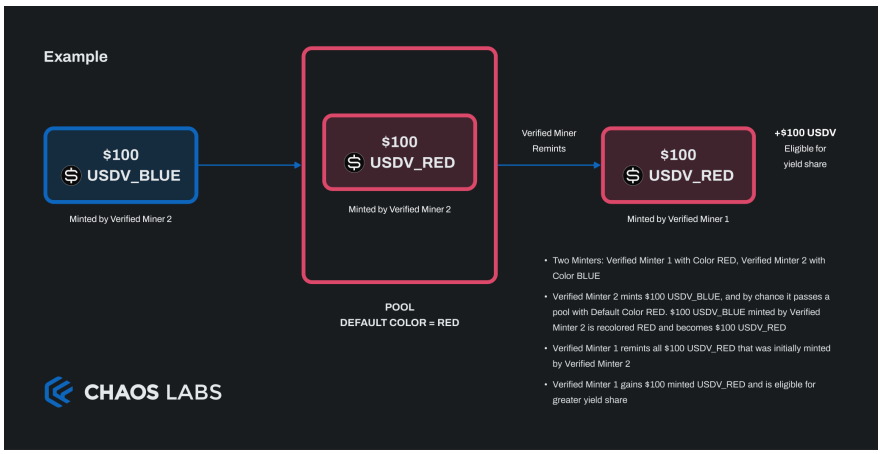


Figure 2.4

2 Reminting and USDV Issuance

Reminting is a permissionless operation that addresses the accumulation of color deltas, allowing the realization of yield potential by reminting more color against others with delta deficits. This Delta-Zero reminting ensures the equilibrium of deltas within the system. The Vault contract oversees USDV issuance, backed by allow listed assets like STBT, facilitating a 1:1 minting process without fees and a redemption mechanism with applicable fees.

2.1 Minting and Redemption Flows

The minting flow is straightforward: STBT owners deposit assets into the Vault, receiving an equivalent amount of USDV and Vault Shares. Conversely, the redemption process allows USDV holders to exchange their tokens for underlying assets, with a portion of the transaction serving as a fee to the operator and the remainder returned to the redeemer along with the removal of corresponding Vault Shares.

2.2 Yield Distribution Mechanics

At the core of USDV's yield distribution lies the globally unique Vault, which houses yield-bearing Tokenized Real World Assets (TRWA) as collateral. The primary asset currently underpinning USDV is the Short-term Treasury Bill Token (STBT), a passive yield-generating asset rebased daily to maintain a 1:1 USD peg. The yield generated is automatically minted into USDV, rewarding Verified Minters for their contributions to the ecosystem.

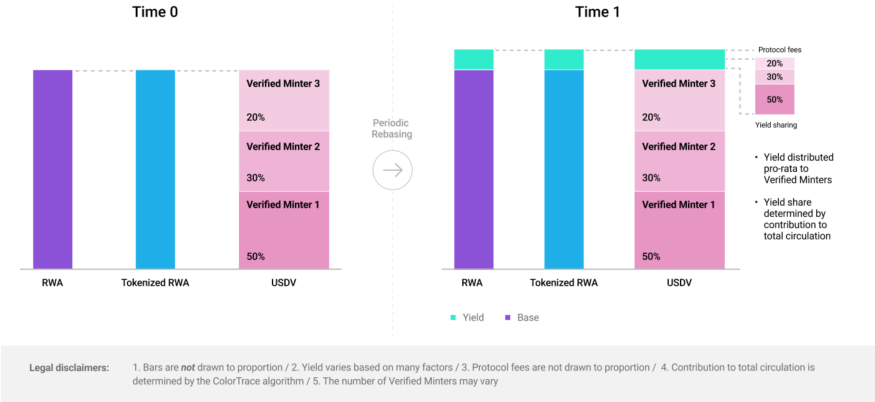


Figure 2.5: Source: USDV Documentation

Fair and Transparent Yield Allocation

The distribution of yield within USDV is both equitable and transparent. Each USDV represents a color share, correlating to a Verified Minter's stake in the global yield pool. Verified Minters are assigned unique Color IDs, which are crucial for directly attributing yield rewards. The global yield is apportioned daily based on the Vault's color shareholdings, with the new USDV stored in the Vault until minters exercise their redemption rights. This process is fully transparent, with all related transactions recorded on-chain for public verification.

Token Value Stability and Assurance

The guarantee of redemption for STBT underpins USDV's value stability. The underlying asset, STBT, is subject to real-time on-chain monitoring, with reserves managed by reputable financial institutions and daily reporting to the USDV Transparency Panel. The Reserve report, verified by a top global accounting firm, ensures that the reserves are always at least equal to the circulating USDV, providing a high level of financial assurance.

3 Fundamental Principles of USDV's Economic Model

- **Enforced Asset Circulation**: This principle ensures that the total number of tokens in circulation is directly tied to the underlying asset holdings. The Vault enforces the creation and destruction of tokens in exchange for these assets, maintaining a global supply invariant.
- **Zero System Error**: The system is designed to maintain a zero net error, with any divergence between the circulation of each color and the mint recorded at the Vault being accurately accounted for. This is encapsulated in the delta-zero invariant, which holds within each domain and system.
- **Mint-Holding Guarantee**: This principle protects minters by ensuring that no operation can reduce their mint below their holdings across all chains. This is achieved by adhering to the delta-zero invariant, with additional restrictions to prevent the reduction of a minter's mint.

3.1 Global Invariants Upholding USDV's Integrity

- **Pegging Invariant**: The global circulation of USDV is always equivalent to the sum of the collateral of all backing assets across all connected chains.
- **Delta-Zero Invariant**: The sum of the deltas of all colors, including Theta (a placeholder for uncolored USDV), on any chain is zero, ensuring a balanced system both locally and globally.
- **Theta-Zero Invariant**: The sum of the deltas of Theta across all chains is zero, maintaining a system-wide balance.
- **Mint Invariant**: The total minted amount of any color across all chains is equal to the Vault shares of that color, ensuring a direct correlation between minting activity and color shareholding.

USDV's mechanism blends economic principles and rigorous assurances. It is crafted to provide a stable, transparent, and fair yield distribution system, underpinned by a robust set of invariants that ensure the integrity and stability of the stablecoin. As we proceed with the risk assessment, we'll analyze potential risks and ensure that the USDV protocol remains resilient against economic and operational challenges.

4 Contract Governance and Risk Management in USDV's Ecosystem

4.1 Contract Governance Structure

The USDV Foundation currently leads USDV's governance. USDV is structured to ensure flexibility and security within its ecosystem. The governance roles are distributed across different entities, each with specific functions to maintain the system's integrity and adaptability.

Vault Governance Roles

- **Operator**: Manages fees, minter registration, color pausing, and rate limit adjustments.
- **Foundation**: Possesses the authority to change the Operator under specific conditions and set the $redemption\_fee\_cap$.
- **Owner**: Responsible for contract upgrades, asset registration, reserve withdrawals, global pausing, and setting various operational parameters.

USDV Token Governance Roles

- **Foundation**: Can blacklist users to prevent minting, burning, or transferring of USDV.
- **Operator**: Handles contract pausing, fee adjustments, and setting color-related parameters.
- **Vault**: Manages minting and burning of USDV.
- **Owner**: Has upgrade authority and role-setting responsibilities.

5 Rate Limiting Mechanisms and Fee Structures

Several rate limiters and fee structures are in place to safeguard the USDV protocol from technical risks and to manage the flow of assets. It is important to note that these parameters and fees are initial and subject to change over time as a function of governance, market demand, security, risk, and additional considerations.

Fee Structure

- **Mint/Redeem Rate Limiter**: This mechanism controls the flow of assets into and out of the system, mitigating the impact of potential technical issues with underlying assets. It operates on a token bucket principle with a defined capacity and refill rate.
- **USDV Redemption Fee**: The operator charges a fee of 10 basis points (bps) for USDV redemptions.
- **Reminting Fee**: The operator charges a fee of 3 bps for the reminting process.

Rate Limit Parameters

- **Cross-chain Rate Limiter**: To manage the risks associated with different blockchain networks, especially newer ones, a rate limiter is applied to control the net outbound flow of USDV, ensuring that any single chain's exposure is kept within safe limits.
- **STBT Minting Limit**: Capped at 100 million USDV with a refill rate of 1,157 USDV per second.
- **STBT Redemption Limit**: Capped at 50 million USDV with a refill rate of 578 USDV per second.

5.1 Additional Governance Functions

- **Liquidity Provider**: Sets the LP Fee for providing liquidity.
- **Donor**: Allows donating backing assets to the vault without minting USDV.

The governance framework of USDV is designed to be robust yet flexible, allowing for the dynamic adjustment of parameters to respond to the evolving DeFi landscape. The risk management protocols are crucial in maintaining the economic stability of the USDV token and protecting it from potential vulnerabilities. These mechanisms work in tandem to ensure that USDV remains a secure and reliable stablecoin within the volatile cryptocurrency market.

Chapter 3

STBT Protocol and Mechanism Design

1 Overview

The advent of USDV, a novel stablecoin, has positioned the Short-term Treasury Bill Token (STBT) at a critical juncture where its role transcends beyond a yield-accruing asset. Anchored on the Ethereum blockchain and in compliance with the ERC-1400 security token standard, STBT now serves as the initial backing asset for USDV. This additional function necessitates an escalated level of scrutiny; the underlying asset's stability, market capitalization, and liquidity impact not only its direct holders but also the broader ecosystem that USDV aims to serve. This STBT risk assessment is predicated on a comprehensive understanding of the emergent context of USDV. A market capitalization surpassing $110 million underscores the criticality of STBT in the digital asset space, where it is daily rebasing to the Net Asset Value (NAV) of its underlying assets, a cornerstone of trust and dependability. The resulting stability is paramount, as any fluctuation in STBT's value or its yield—currently in the vicinity of 4 to 5 percent APY—directly affects the peg and the perceived reliability of USDV. The report delineates STBT's operational framework, reserve management strategies, compliance protocols, and market behaviors. The operational oversight by Matrixdock is crucial, as it ensures that the STBT is robust in its standing and as a backing asset for USDV. The dual utility of STBT amplifies the importance of understanding and mitigating its associated risks—contractual, operational, liquidity, oracle, depegging, and regulatory—which now have compounded effects on the USDV ecosystem. This report aims to provide a nuanced analysis of STBT within the USDV context, equipping stakeholders with information critical to their decision-making. The insights will guide investors, regulators, and the DeFi community, helping them comprehend the implications of STBT's performance as a backing asset and its broader impact on the stability and adoption of USDV.

2 Treasury Bill Backing

The Short-term Treasury Bill Token (STBT) architecture is a confluence of well-established financial principles and the innovative underpinnings of blockchain technology. This section delineates the operational framework and structural components of STBT, elucidating how

it functions as both an investment asset and as the bedrock for the USDV stablecoin.

Overview of US Short-Term Treasury Bills

6-month T-bills, or 6-month Treasury bills, are short-term debt securities issued by the U.S. Department of the Treasury. They are a type of government bond with a maturity period of six months. Investors purchase these T-bills at a discount to the face value, and the difference represents the interest earned at maturity. T-bills are considered low-risk investments often used by investors as a short-term, safe-haven asset.

Custody and Management of Treasury Bills

T-bills custodianship refers to the safekeeping and management of Treasury bills by a custodian, typically a financial institution. Custodians are crucial in handling the administrative tasks associated with T-bill ownership, including safe storage, transaction settlement, and record-keeping.

The importance of T-bill custodianship lies in providing a secure and efficient way for investors to manage their Treasury bill investments. Custodians ensure the safe storage of physical or electronic T-bill certificates, handle transactions, and provide investors with accurate and up-to-date information on their holdings. This service simplifies investment, enhances transparency, and helps investors monitor and manage their T-bill portfolios effectively.

Valuation of U.S. Short-Term Treasury Bills

The valuation of U.S. Short-Term Treasury Bills (T-Bills) is determined by the demand for low-risk, liquid, and short-term debt instruments issued by the United States Department of the Treasury. T-bills are typically issued with maturities of four weeks (one month), eight weeks (two months), thirteen weeks (three months), twenty-six weeks (six months), and fifty-two weeks (one year). They are sold at a discount to their face value, and upon maturity, the government pays the holder the total face value. The difference between the purchase price and the face value represents the interest earned by the investor.

The yield of T-Bills is a widely observed indicator of short-term interest rates. Monetary policy, inflation expectations, and the overall demand for safe assets influence it. In times of economic uncertainty or market stress, investors often flock to T-Bills, increasing their prices and consequently lowering their yields due to their perceived safety (a phenomenon known as a "flight to quality").

Volatility of U.S. Short-Term Treasury Bills

Despite being considered one of the safest investment vehicles, T-Bills are not entirely free from volatility. Factors that can induce volatility include:

- **Monetary Policy Changes**: Decisions by the Federal Reserve on interest rates can directly influence T-bills yields.
- **Inflation Expectations**: Higher inflation can erode the purchasing power of the fixed returns from T-Bills, affecting their attractiveness to investors.

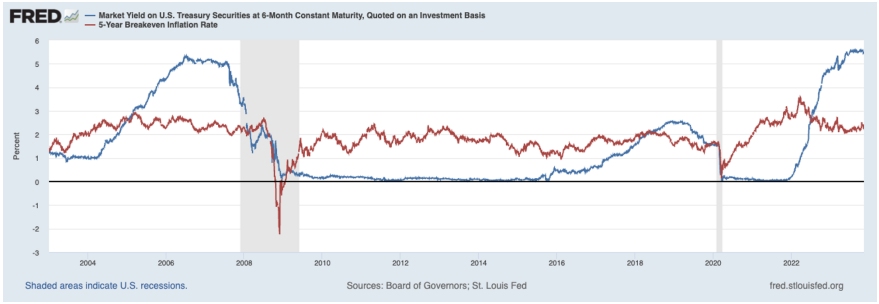


Figure 3.1: 6-Month T-Bills interest rates (blue) compared with 5-Year Break-Even Inflation Rate. The breakeven inflation rate represents a measure of expected inflation derived from 5-year Treasury Constant Maturity Securities and 5-year Treasury Inflation-Indexed Constant Maturity Securities.

- **Government Debt Levels**: Large amounts of T-Bill issuance to finance government spending can influence supply and demand dynamics.
- **Global Market Dynamics**: In a globally connected financial system, international events can cause investors to adjust their holdings in T-Bills, affecting their prices and yields.
- **Creditworthiness of the U.S. Government**: Although extremely rare, any event that leads investors to question the creditworthiness of the U.S. government could result in volatility.

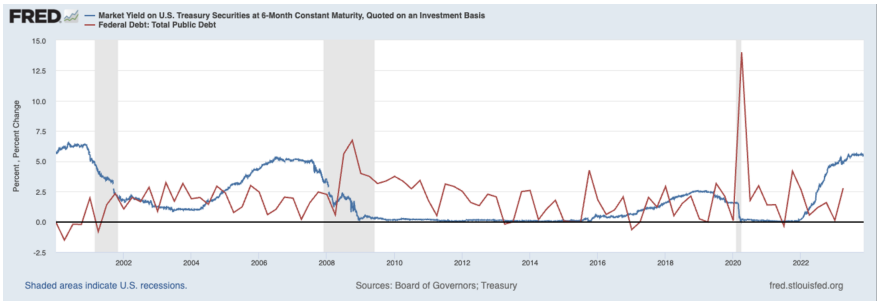


Figure 3.2: 6-Month T-Bills interest rates (blue) compared with the percent change in Federal Total Public Debt.

2.1 Reverse Repurchase Agreements

Temporary open market operations involve short-term and reverse repurchase agreements designed to temporarily add or drain reserves available to the banking system and influence day-to-day trading in the federal funds market.

A reverse repurchase agreement (known as reverse repo or RRP) is a transaction in which the New York Fed, under the authorization and direction of the Federal Open Market Committee, sells a security to an eligible counterparty with an agreement to repurchase that same security at a specified price at a specific time in the future. For these transactions, eligible securities are U.S. Treasury instruments.

Exposure to reverse repos is similar to holding 6-month Treasury bills because both are considered low-risk, short-term investments. Both provide a source of liquidity and are often used by financial institutions to manage cash flow.

The main difference lies in the instruments. Reverse repos involve a contractual agreement and typically a broader range of securities, while 6-month T-bills are specific government-issued debt securities with a fixed term of six months. In both cases, market conditions, interest rates, and the counterparties' creditworthiness influence the risk exposure.

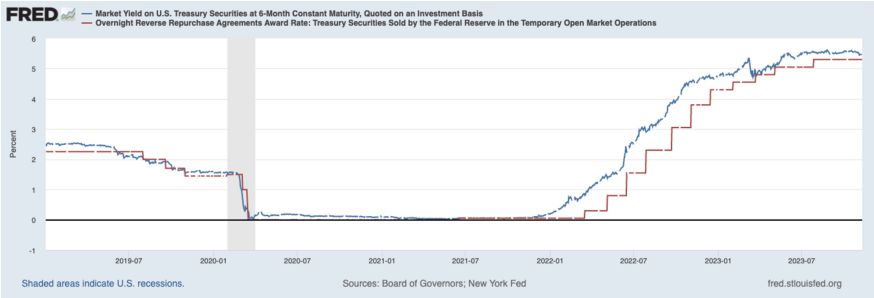


Figure 3.3: 6-Month T-Bills interest rates (blue) compared with Overnight Reverse Repo Agreements Award Rate. The award rate is given to all accepted propositions for the collateral type reported by the New York Fed as part of the Temporary Open Market Operations.

2.2 Conclusion

While U.S. Short-Term Treasury Bills are a cornerstone of financial stability and a benchmark for short-term interest rates, they are not immune to volatility. The valuation and yields of T-Bills can fluctuate due to macroeconomic policies, fiscal dynamics, and shifts in investor sentiment. For stablecoins like USDV backed by instruments such as STBTs, the intrinsic stability of T-Bills is favorable, but it is still critical to recognize and prepare for potential volatility in these underlying assets. As such, strategies to mitigate exposure to T-Bill volatility should be considered in the overall risk management framework for such stablecoins.

3 Governance and Management

The governance and management of the Short-term Treasury Bill Token (STBT) are crucial for maintaining its structural integrity, operational efficacy, and regulatory compliance. These elements collectively ensure that the token operates within the confines of established financial regulations and meets the expectations of its stakeholders. Here, we dissect the

intricate governance frameworks and management protocols that oversee the STBT's day-to-day operations and long-term strategic direction.

3.1 Trust Structure and Issuance

At the heart of STBT's governance is a specialized trust structure designed to safeguard the interests of token holders and ensure compliance with applicable laws and regulations. The trust is responsible for issuing STBT, which is conducted under a stringent regulatory framework to prevent fraudulent activities and protect investors. The trust structure is not a mere formality but a foundation that ensures the token's credibility and legitimacy in the financial market. It is particularly critical given its role in underpinning the USDV stablecoin.

3.2 Operational Management by Matrixdock

Matrixdock is pivotal in managing STBT's daily operations, executing the rebase mechanism, managing reserve assets, and overseeing integration with DeFi applications like Curve. Matrixdock's role extends to enforcing the trust's policies, managing the issuance and redemption processes, and ensuring that the token's operations adhere to the trust's governance protocols. Their operational leadership is essential in maintaining the STBT's functionality and reliability.

3.3 Specialized Trust Structure

The trust structure of the Short-term Treasury Bill Token (STBT) reflects a sophisticated and secure approach to managing and operating this innovative financial instrument.

3.4 Service Provider: Matrixdock

- **Operational Management**: Matrixdock, a subsidiary of Matrixport, is entrusted with the operational management of STBT. Matrixport, established in 2019, is a reputable crypto financial services company with a custody of over $6 billion in assets.
- **Product Innovation**: STBT represents Matrixdock's inaugural venture into yield tokenization products, marking a significant step in the company's expansion into the digital asset space.

3.5 Parent Company: Matrix Finance and Technologies Holdings

- **Robust Structure**: The parent company has meticulously structured STBT within a specialized trust. This involves separating the token-issuing entity (Prometheus Solutions Ltd.) and the asset-holding entity (Epimetheus Technologies SPC).
- **Orphan Trust Structure**: The arrangement is such that these entities are securely nested within the trust, with Appleby Global Services as the trust's guardian and Hamilton Services overseeing trustee activities. This structure ensures that STBT entities remain distinct from Matrixdock's financial overview, safeguarding against claims in the event of Matrixdock's financial adversities.

3.6 Operational Blueprint: Orphan SPV Structure

- **Traditional Finance Parallel**: The STBT operational model mirrors traditional finance's orphan Special Purpose Vehicle (SPV) structure. This mechanism is prevalent in asset-backed and mortgage-backed securities issuance.
- **Potential for High Ratings**: Given the appropriate financial structuring, similar mechanisms support over $1 trillion in global securities and can achieve AAA ratings. STBT's foundation on assets with top-tier creditworthiness, backed by the U.S. government, enhances its credibility.

3.7 Reserves Management

- **Collateral Composition**: STBT is collateralized by short-term U.S. Treasury bills and reverse repurchase agreements. With maturities of six months or less and overnight reverse repos, the T-bills provide exposure to short-term U.S. interest rates while minimizing duration risk.
- **Proof-of-Reserve**: Matrixdock issues daily proof-of-reserve statements detailing the distribution between T-bills and reverse repo assets. This transparency is crucial in maintaining the trust and credibility of the STBT.
- **Allocation Strategy**: The current allocation is approximately 90% in reverse repos and 10% in T-bills. This strategy is aligned with the yield curve dynamics and the project's early developmental stage.
- **Disclosure of Underlying Assets**: The verifications include the CUSIP number of the treasuries, details of the repo agreements, and the market value of the underlying assets, ensuring complete transparency in the reserve management.

3.8 Geographic Restrictions

Matrixdock, the entity responsible for the operational management of STBT, adheres to regulatory guidelines, which entail not offering services in specific regions due to varying interpretations of securities law across jurisdictions. The regions where Matrixdock refrains from offering STBT include:

- **Asia**: Mainland China, retail clients from Hong Kong, Singapore, North Korea, Japan, Iran, Syria, and Myanmar.
- **Americas**: USA, Canada, American Samoa, Cuba, Guam, Puerto Rico, and the Northern Mariana Islands.
- **Europe**: Crimea, Sevastopol, and Russia.

For each client onboarded, careful consideration is given to their place of incorporation or residence to determine the local rules for selling them a security token on an exempt basis. Explicitly, Matrixdock does not sell to US persons, adhering instead to a global standard that is often benchmarked to the United States stringent regulations.

3.9 Legal Frameworks

Regarding legal frameworks, the STBT falls under the purview of the laws of Seychelles, where its specialized trust is incorporated. The Securities Act 2007 is the main legislation overseeing securities and investment products in Seychelles, with the Financial Services Authority (FSA) being the designated regulatory entity for securities dealers, investment advisers, and exchanges. Notably, the Securities Act does not classify virtual assets or cryptocurrencies as securities, and the classification depends on the specific characteristics of the asset.

Matrixdock has secured a legal opinion from a reputable Seychelles-based law firm confirming that the STBT offering does not qualify as an investment business under Seychelles legislation and, thus, does not fall under the regulations of the FSA. However, when extending offerings to nationals of third countries, the reverse solicitation principle is employed, which must be navigated carefully due to potential shifts in regulatory interpretation.

Furthermore, in jurisdictions like the UK and EU, Matrixdock has consulted with major law firms to understand the relevant exemptions for the offer and sale of unregistered securities like STBT, and these standards are applied in each transaction to ensure compliance.

These frameworks and restrictions underscore the complex legal landscape that Matrixdock navigates to maintain the compliant distribution of STBT, which is essential not only for its functionality as a yield token but also for its role as the backing asset for the USDV stablecoin. The proactive approach to compliance demonstrates a commitment to aligning with the intricate and dynamic legal landscape, which is critical for the credibility and sustainability of STBT and USDV.

3.10 AML and KYC Policies

The Anti-Money Laundering and Know Your Customer policies for the Short-term Treasury Bill Token (STBT) are integral to its governance and risk management framework. These policies ensure that the operations adhere to regulatory standards to prevent financial crimes such as money laundering and terrorist financing.

AML Policies

The AML procedures for STBT are designed to monitor and prevent any transactions involving the proceeds of crime. As part of the broader AML framework, Matrixdock, the operational manager of STBT, implements systems and controls that include:

- **Due Diligence**: Conducting thorough due diligence on all customers to understand their activities' nature and assess the risk of money laundering.
- **Transaction Monitoring**: Continuous monitoring of customer transactions to identify and report any suspicious per applicable laws and regulations.
- **Record Keeping**: Maintaining detailed records of customer identities, transactions, and risk assessments, as regulatory authorities require.

KYC Policies

The KYC process is a critical step for all potential STBT investors. This process involves several key components:

- **Identity Verification**: Investors must provide sufficient documentation to verify their identity, which may include government-issued identification and proof of address.
- **Accreditation Verification**: As STBT targets accredited investors, additional documentation may be required to establish this status, such as financial statements or certifications from a financial advisor.
- **Risk Assessment**: Each customer is assessed for risk based on the information provided, which helps to tailor the monitoring of their transactions and activities.
- **Whitelisting**: Following the KYC and risk assessment, approved investors are added to a whitelist that allows them to participate in STBT transactions. This whitelist ensures that only verified and approved investors can transfer STBT tokens, enhancing the overall security and compliance posture.

Matrixdock undertakes these AML and KYC processes to comply with the prevailing financial regulations and maintain the STBT ecosystem's integrity. This is paramount not just for the operation of STBT but also for maintaining the stability and credibility of USDV, which relies on STBT as its primary collateral. The AML and KYC policies are designed to be robust and adaptable to the evolving regulatory environment, ensuring that STBT can fulfill its role as a backing asset for USDV while mitigating financial crime risks.

4 Service Providers

The custodians and broker-dealer pricing providers play an integral role in the operational framework of the Short-term Treasury Bill Token (STBT), ensuring the security and proper valuation of the assets underlying the token. Here is a detailed description of their roles and responsibilities:

4.1 Custodians

The custodian(s) hold the T-bill and reverse repo collateral in custody accounts under contract with Epimetheus Technologies SPC, the asset-holding entity under the STBT special purpose trust. The custodians are crucial to ensuring the safekeeping of the assets that back the STBT, providing a layer of security for token holders. Due to regulatory sensitivity and the desire for confidentiality in the banking sector, especially concerning associations with crypto companies, the names of these custodians are not disclosed publicly. However, Matrixdock has confirmed that their custodial partners are reputable institutions, and this information has been shared privately with the necessary parties.

4.2 Broker-Dealer

A broker-dealer is contracted to engage in the reverse repo transactions backed by T-bills, which is crucial in managing the collateral's liquidity and yield generation. Like the custodians, the service provider acting as the broker-dealer is not disclosed publicly due to the potential regulatory implications and the need for discretion in the financial services industry.

4.3 Pricing Providers

Bloomberg is utilized as the pricing data provider to determine the net asset value and trigger STBT rebates accurately. The daily closing prices provided by Bloomberg are essential for accurately calculating the STBT's NAV, used in the daily rebasing process. This pricing information is a critical component of the rebase mechanism, as it ensures that the token supply is correctly adjusted to reflect the actual value of the underlying assets.

4.4 Proof of Reserves

The Proof of Reserves (PoR) system is a pivotal component of the Short-term Treasury Bill Token (STBT) ecosystem. It is a transparency mechanism, providing stakeholders with verifiable evidence of the collateral backing STBT. Matrixdock utilizes Chainlink's Proof of Reserve service. Chainlink offers an Oracle which write the results of The Network Firm LLP's daily account statement verifications. Let's review each distinct yet complementary role.

Role of Chainlink

- **Data Oracles**: Chainlink operates as the data oracle provider within the STBT ecosystem. Its primary function is to validate the reserves' valuation externally.
- **Real-Time Updates**: Leveraging its decentralized network of nodes, Chainlink ensures real-time and accurate updates of reserve values, feeding this information into the STBT smart contracts.
- **Transparency and Security**: Chainlink's integration enhances the security and transparency of the PoR system by providing decentralized validation. Chainlink works with The Network Firm as a third-party account statement verifier.

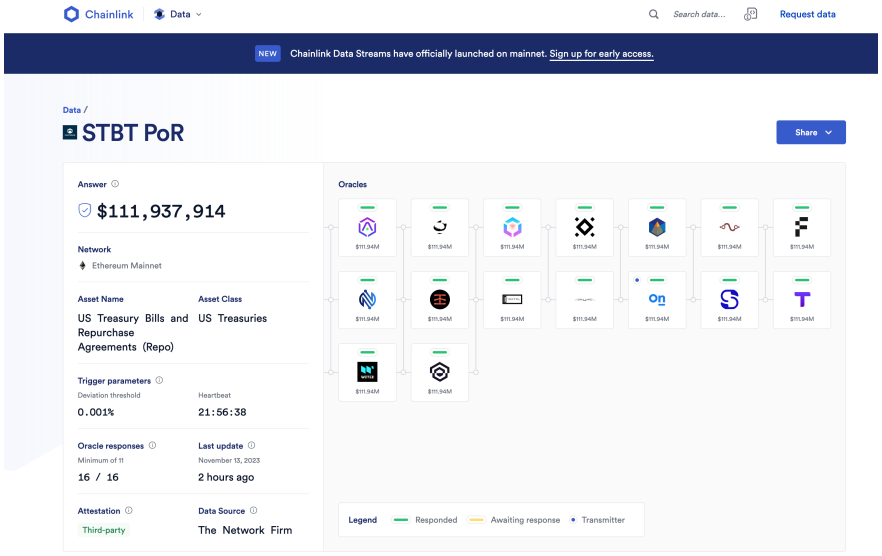


Figure 3.4: For real-time Proof of Reserves, visit the Chainlink Dashboard.

Role of the Network Firm LLP

- **Independent Assessment of Custodian Statements**: The Network Firm LLP is a service provider to Chainlink, and independently checks the STBT's reserve holding statements, as part of the Proof of Reserve product. This is crucial for verifying the integrity and accuracy of the reported values.
- **Daily Verification**: The firm provides regular verifications confirming the existence and valuation of the reserve assets, reinforcing the trust in the STBT's backing.
- **Compliance**: Their involvement ensures that the PoR adheres to regulatory standards and accounting principles, offering a layer of financial diligence and compliance.

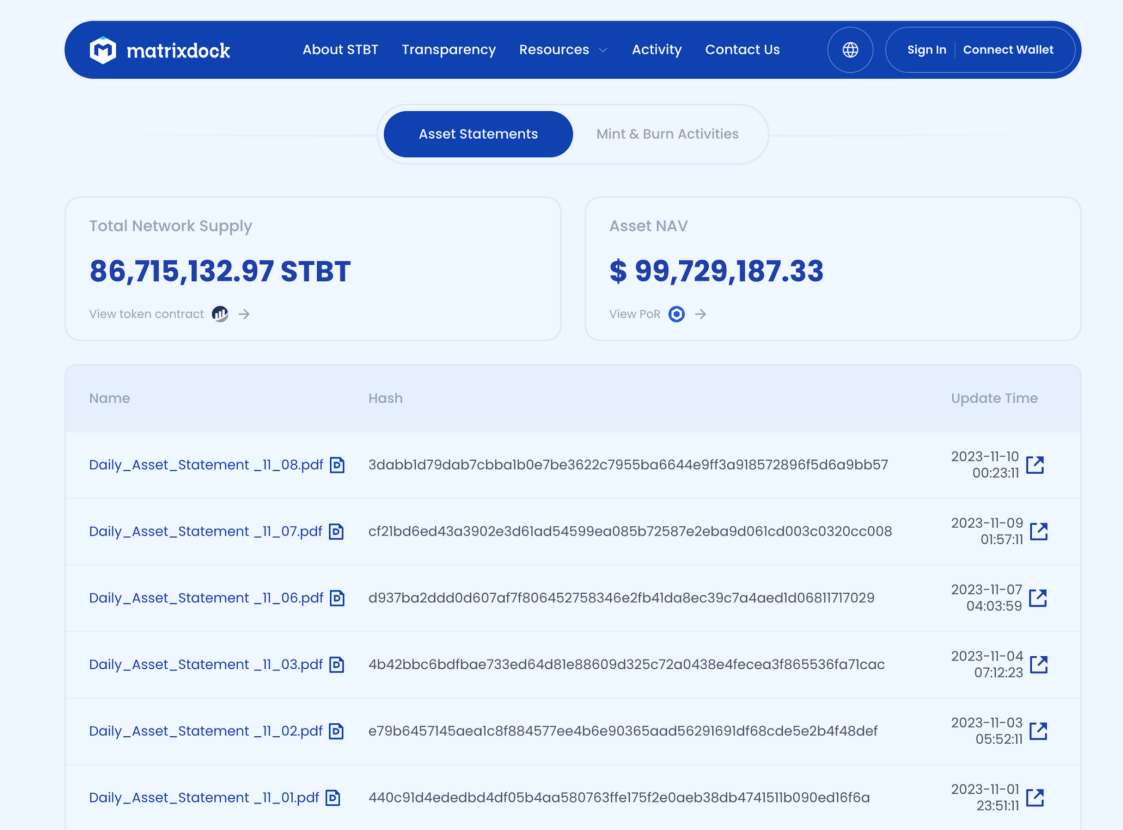
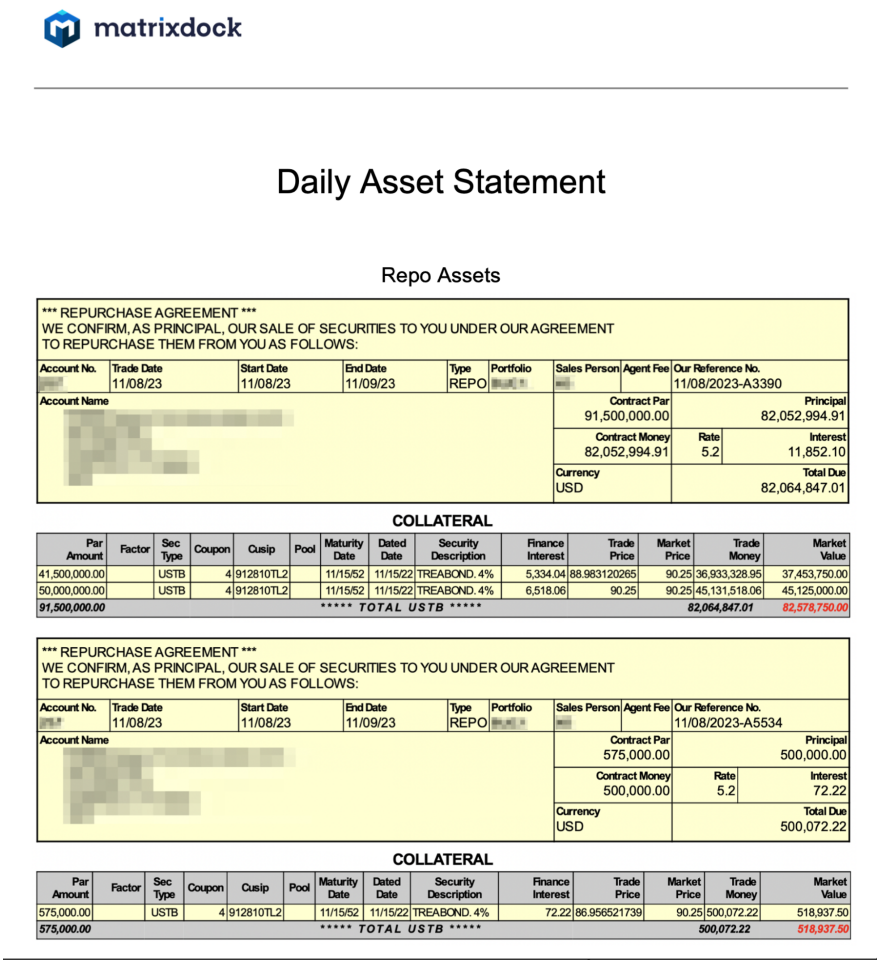


Figure 3.5: Daily Proof of Reserves (PoR) Attestation: This screenshot captures the latest PoR attestation, showcasing the current distribution and valuation of STBT's reserve assets, as maintained and reported by Matrixdock. These are updated daily and can be viewed on the Matrixdock Transparency tab.

Role of Matrixdock

- **Operational Oversight**: Matrixdock, responsible for the operational management of STBT, plays a crucial role in maintaining and reporting the PoR.
- **Daily Statements**: Matrixdock works with a third-party custodian, which releases daily PoR statements, including detailed information about the STBT's reserve assets.

- **Collaboration and Integration**: The Network Firm verifies daily account statements and provides the results of the verification via API for Chainlink. Chainlink PoR Oracle Feeds then write the results of the daily verification on-chain.



matrixdock

Daily Asset Statement

Repo Assets

*** REPURCHASE AGREEMENT ***
WE CONFIRM, AS PRINCIPAL, OUR SALE OF SECURITIES TO YOU UNDER OUR AGREEMENT
TO REPURCHASE THEM FROM YOU AS FOLLOWS:

Account No.	Trade Date	Start Date	End Date	Type	Portfolio	Sales Person	Agent Fee	Our Reference No.
	11/08/23	11/08/23	11/09/23	REPO				11/08/2023-A3390

Account Name

Contract Par	Principal
91,500,000.00	82,052,994.91
Contract Money	**Rate** / **Interest**
82,052,994.91	5.2 / 11,852.10
Currency	**Total Due**
USD	82,064,847.01

COLLATERAL

Par Amount	Factor	Sec Type	Coupon	Cusip	Pool	Maturity Date	Dated Date	Security Description	Finance Interest	Trade Price	Market Price	Trade Money	Market Value
41,500,000.00		USTB	4	912810TL2		11/15/52	11/15/22	TREABOND. 4%	5,334.04	88.983120265	90.25	36,933,328.95	37,453,750.00
50,000,000.00		USTB	4	912810TL2		11/15/52	11/15/22	TREABOND. 4%	6,518.06	90.25	90.25	45,131,518.06	45,125,000.00
91,500,000.00						***** TOTAL USTB *****						***82,064,847.01***	***82,578,750.00***

*** REPURCHASE AGREEMENT ***
WE CONFIRM, AS PRINCIPAL, OUR SALE OF SECURITIES TO YOU UNDER OUR AGREEMENT
TO REPURCHASE THEM FROM YOU AS FOLLOWS:

Account No.	Trade Date	Start Date	End Date	Type	Portfolio	Sales Person	Agent Fee	Our Reference No.
	11/08/23	11/08/23	11/09/23	REPO				11/08/2023-A5534

Account Name

Contract Par	Principal
575,000.00	500,000.00
Contract Money	**Rate** / **Interest**
500,000.00	5.2 / 72.22
Currency	**Total Due**
USD	500,072.22

COLLATERAL

Par Amount	Factor	Sec Type	Coupon	Cusip	Pool	Maturity Date	Dated Date	Security Description	Finance Interest	Trade Price	Market Price	Trade Money	Market Value
575,000.00		USTB	4	912810TL2		11/15/52	11/15/22	TREABOND. 4%	72.22	86.956521739	90.25	500,072.22	518,937.50
575,000.00						***** TOTAL USTB *****						***500,072.22***	***518,937.50***

Figure 3.6: Network Firm's Daily Statement: The recent daily statement verification by the Network Firm LLP provides an independent verification of STBT's reserve holdings, ensuring transparency and compliance with regulatory standards.

Third-party auditing is essential to validate the asset holdings' integrity and assure token holders regarding the backing of the STBT.

5 Fee Structure

The fee structure associated with the Short-term Treasury Bill Token (STBT) is designed to cover operational costs, maintain the system's integrity, and provide services efficiently. Here, we delineate the various types of fees associated with STBT:

5.1 Issuance and Redemption Fees

- **Redemption Fees**: 0.1% fee, based on redemption value, applied when STBT tokens are redeemed for their underlying assets; these fees are meant to manage the costs

associated with liquidating assets and processing the redemption.

5.2 Custodial Fees

- **Purpose**: Custodial fees are levied to compensate for the safekeeping and management of the underlying assets (U.S. Treasury bills and reverse repurchase agreements) held in custody.
- **Custodian Role**: These fees are paid to third-party custodians who ensure the security and regulatory compliance of the assets backing the STBT.

5.3 Reverse Repo Brokerage Fees

- **Brokerage Services**: Fees associated with the brokerage services for engaging in reverse repurchase agreements.
- **Risk Management**: These fees contribute to the risk management and operational execution of reverse repo transactions.

5.4 Matrixdock Service Fees

- **Management Services**: Matrixdock, as the operational manager of STBT, charges service fees of 0.1% per annum on the notional amount of STBT for its management and administrative services.

6 Protocol and Mechanism Design

6.1 ERC-1400 Security Token Standard Compliance

STBT is engineered within the strictures of the ERC-1400 standard, which stipulates a stringent set of criteria for security tokens on the Ethereum blockchain. This standard ensures that STBT maintains essential security features, such as compliance with regulatory directives, enhanced investor protections, and robust token recovery mechanisms. Adhering to such rigorous standards indicates the token's commitment to security and regulatory compliance, which is paramount given its foundational role for USDV.

6.2 STBT Minting

The Short-term Treasury Bill Token (STBT) features structured processes for minting and redemption, each encompassing various stages, associated risks, and potential timeframes. Below is a detailed overview of these processes:

Initiation

- **Stage**: Investors or entities initiate minting by depositing an equivalent value of recognized stablecoins.
- **Timeframe**: Depending on transaction processing and verification, this stage may take a few hours to a day.

- **Risk**: Delays or errors in deposit verification.

Token Generation

- **Stage**: STBT tokens are minted to correspond with the deposited value upon successful verification.
- **Timeframe**: Typically completed within minutes.
- **Risk**: Smart contract vulnerabilities could lead to minting errors.

Distribution

- **Stage**: Minted STBT tokens are distributed to the investor's wallet.
- **Timeframe**: Instantaneous post-minting.
- **Risk**: Delays or failures in token transfer due to network congestion.

6.3 STBT Redemption

Redemption Request

- **Stage**: Token holders initiate a redemption request for their STBT tokens.
- **Timeframe**: Can range from a few minutes to hours, depending on system efficiency.
- **Risk**: Operational delays or request processing errors.

Asset Liquidation

- **Stage**: The equivalent underlying assets (U.S. Treasury bills or reverse repo contracts) are liquidated to match the redemption value.
- **Timeframe**: This process can take a few hours to a few days, depending on market conditions and asset liquidity.
- **Risk**: Market volatility affecting the liquidation value; liquidity constraints.

Fund Transfer

- **Stage**: The corresponding value is transferred to the investor in stablecoins or fiat currency.
- **Timeframe**: Usually completed within the same day of liquidation.
- **Risk**: Transfer delays due to banking or blockchain network issues.

Token Burn

- **Stage**: Redeemed STBT tokens are burned or removed from circulation.
- **Timeframe**: Instantaneous upon successful transfer completion.
- **Risk**: Technical issues in the token burning process.

Minting and Redemption Risk

- **Market Conditions**: Fluctuations in the market can affect both the minting (valuation of T-bills and reverse repos) and redemption (asset liquidation value) processes.
- **Regulatory Compliance**: Ensuring compliance with financial regulations may introduce delays in minting and redemption processes.
- **Operational Efficiency**: The overall efficiency of MatrixDock in managing these processes can significantly impact the timeframe of each stage.

7 Rebasing Mechanism

The rebasing process of Short-term Treasury Bill Token (STBT) is a critical mechanism designed to align the total supply of STBT with the Net Asset Value (NAV) of its underlying assets. This section elaborates on the rebasing flow, incorporating the provided information and additional insights.

- **Daily Adjustment**: STBT's total supply undergoes a rebase daily, adjusted to match the NAV of the underlying U.S. Treasury bills and reverse repurchase agreements.
- **Pricing Data Utilization**: Matrixdock employs Bloomberg pricing data for rebase calculations, explicitly referencing the 3 p.m. New York time closing price. The fair market value of the T-bills and reverse repos is determined using Bloomberg's historical prices (HP) function and the Bloomberg Generic (BGN) price source.

7.1 Rebasing Formula

The formula used for determining the daily interest distribution through rebasing is as follows:

$$DailyInterestDistributed = NAVofCurrentDay - NAVofLastRebaseDay - Expenses$$

Where:

- **NAV of Current Day** - The net asset value of the underlying assets on the current day.
- **NAV of Last Rebase Day** - The net asset value of the underlying assets on the previous rebase day.
- **Expenses** - These include the T-bill Custodian Fee, Reverse Repo Brokerage Fee, and Matrixdock Service Fee, with an estimated annual fee of approximately 0.3% per annum.

7.2 Example

Suppose the NAV of the underlying assets on the current day is \$1,000,000, and the NAV on the last rebase day was \$995,000. If the total expenses amount to \$1,500, then the daily interest distributed through rebasing would be:

\$1,000,000 - \$995,000 \$1,500 = \$3,500

This \$3,500 represents the new STBT minted and distributed to holders.

7.3 Risks - Market Volatility

While rare, fluctuations in the T-bill market can lead to decreased NAV. In such cases, rebasing is paused until the NAV rebounds above the last rebase point.

7.4 Risks - Valuation Accuracy

Dependence on Bloomberg's pricing data necessitates accurately valuing the underlying assets. Any discrepancies in pricing data can affect the rebasing outcome.

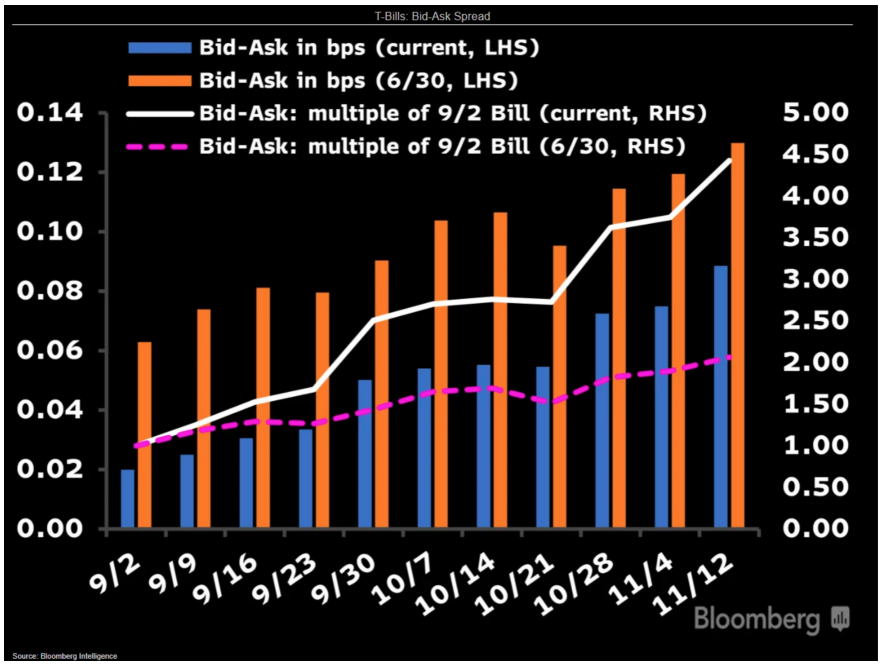


Figure 3.7: TBill Bid-Ask Spread. Source: Bloomberg

7.5 Risks - Operational Dependence

The rebasing model relies on active management by Matrixdock, making operational efficiency and accuracy crucial.

8 Redemption Pricing and Execution

8.1 Redemption Pricing

The pricing of redemptions for the Short-term Treasury Bill Token (STBT) is based on the underlying assets' Net Asset Value (NAV). The NAV represents the per-token value of the STBT and is calculated by dividing the total value of the underlying treasury bills and reverse repurchase agreements by the total number of STBT tokens in circulation.

For an investor looking to redeem STBT tokens, the redemption price would be the current NAV when the redemption request is processed. This price should reflect any accrued interest on the underlying assets until the redemption date. The pricing mechanism ensures that investors receive a fair value for their tokens that directly corresponds to the market value of the collateralized assets.

8.2 Execution of Redemptions

The execution process for redemptions involves several steps:

- **Redemption Request**: Investors initiate a redemption request through the platform or service designated by Matrixdock.
- **Verification**: The request is verified against the investor's holdings and their eligibility for redemption.
- **Locking in the Price**: The NAV locks in the redemption price at the time of the request, subject to daily cut-off times.
- **Settlement Period**: There is typically a settlement period during which the assets are liquidated to provide the cash equivalent of the redemption value. The length of this period can vary but is often predefined to manage liquidity expectations.
- **Transfer of Funds**: Once the underlying assets are liquidated, the equivalent value is transferred to the investor, completing the redemption process. The transfer may be made in the form of stablecoins or the fiat currency equivalent, depending on the terms set by Matrixdock.

8.3 Market Impact Considerations

Redemptions are executed with consideration of their potential impact on the market. Large redemption orders may be processed in tranches to avoid disrupting the market price of the underlying assets, especially if the liquidity in the market is low at the time of redemption.

8.4 Fees and Charges

Investors may be subject to fees deducted from the redemption value. These can include transaction fees, operational costs, and any other fees Matrixdock stipulates.

8.5 Redemption Risks

The process of redeeming STBT tokens for their underlying value is a critical aspect of the token's liquidity and investor confidence. However, this mechanism has inherent risks, which can impact both the token and its holders.

8.6 Market Impact Risk

Large-scale redemptions can exert downward pressure on the price of STBT if the process involves selling underlying assets in the open market. This selling activity could lead to an imbalance in supply and demand, potentially resulting in a reduced value of the tokens if the market can only absorb the sales with price concessions.

Note: Market impact risk for STBT is considerably low, given that U.S. Treasury Bills constitute a multi-trillion-dollar market, ensuring that any selling activities by STBT, even at significant volumes, are unlikely to impact the overall market due to its depth.

8.7 Liquidity Risk

STBT's liquidity is anchored on the premise that the underlying assets, namely short-term U.S. Treasury bills and reverse repurchase agreements, can be readily converted into cash to meet redemption requests. However, in times of market stress or liquidity crunches, the ability to liquidate these assets quickly and without significant loss of value can be compromised, posing a liquidity risk to the token.

Note: Liquidity risk for STBT is considerably low, given that U.S. Treasury Bills constitute a highly liquid multi-trillion-dollar market, ensuring that any selling activities by STBT, even at substantial volumes, are unlikely to significantly influence the overall market due to its vast liquidity and depth.

8.8 Operational Risk

The mechanics of processing redemptions involve various operational components, including transaction verification, execution of sales for liquidity, and transfer of value to the redeemer. Failures or errors in this operational chain can lead to delays or financial losses, undermining the redemption process's reliability.

8.9 Concentration Risk

If a few holders have large concentrations of STBT, their redeeming decisions could significantly impact the token's overall on-chain liquidity profile. This concentration risk could lead to increased volatility and potentially destabilize the token if these large holders were to redeem their positions simultaneously.

8.10 Regulatory Risk

Changes in regulatory frameworks can affect the redemption process, especially if new regulations alter the liquidity of underlying assets or the legal procedures for redemption. STBT operates in a complex regulatory environment, which can evolve and introduce new challenges to the redemption mechanism.

8.11 Counterparty Risk

In reverse repurchase agreements, a counterparty risk is associated with the entities on the other side of these transactions. A counterparty failing to honor its obligations could impact the ability to meet redemption requests promptly and efficiently.

8.12 Mitigation Strategies

To mitigate these risks, STBT's management must employ prudent reserve management, maintain a diversified liquidity pool, establish robust operational procedures, and continuously monitor regulatory developments. Additionally, having contingency plans in place to address large, unexpected redemptions can help manage and distribute the associated risks more effectively.

8.13 Transparency and Reporting

Transparency in the redemption process is maintained through regular reporting and disclosure of redemption activities. This may include the volume of redemptions, the NAV calculations, and any changes to the fees or execution process.

9 Bloomberg Pricing and Oracle Reliability

9.1 Reliance on Bloomberg for Asset Pricing

The Short-term Treasury Bill Token (STBT) relies on Bloomberg's reputable pricing services to provide accurate and up-to-date valuation data for the underlying assets. Bloomberg's service is widely recognized for its market data accuracy, which includes real-time and historical data across various asset classes, including U.S. Treasury bills and reverse repurchase agreements. This pricing data is crucial for the daily rebasing of STBT, ensuring that the token's supply accurately reflects the underlying assets' Net Asset Value (NAV).

9.2 DeFi Integrations

STBT's integration with Curve, a decentralized exchange for stablecoins, serves as its genesis integration. Curve facilitates efficient token swaps with low slippage, crucial for maintaining STBT's liquidity. This integration is not merely a technicality but a strategic move to ensure that market liquidity for STBT is sustained, providing a reliable avenue for token exchange and price stability. This functionality is especially significant for STBT's role in underpinning USDV, where liquidity is tantamount to the stablecoin's ability to maintain its peg.

9.3 Oracle Integration for Data Feeds

STBT integrates with Bloomberg's pricing data through an Oracle system. Oracles are third-party services that feed external data into the blockchain to trigger smart contract executions—in this case, the daily rebasing of STBT. The integrity and reliability of this oracle system are paramount, as any inaccuracies in data feed or delays in data transmission can lead to improper rebasing actions.

9.4 Data and Oracle Security and Risk Vectors

Despite Bloomberg's strong reputation, the integration of its pricing data into STBT's smart contracts presents several security considerations:

1. **Data Integrity Risk**: The risk that the pricing data provided by Bloomberg could be incorrect due to a technical malfunction, human error, or deliberate manipulation.
2. **Oracle Manipulation Risk**: The potential for bad actors to exploit vulnerabilities in the Oracle system to feed false data to the smart contracts, potentially leading to erroneous rebasing.
3. **Centralization Risk**: Reliance on a single pricing source introduces centralization risk, where the failure or compromise of Bloomberg's data feed could disrupt STBT's operations.

To mitigate these risks, STBT's oracle integration must employ robust security measures, including:

- **Multiple Data Sources**: Using data from multiple providers to prevent single points of failure.
- **Data Verification Protocols**: Implementing verification mechanisms to cross-check data before it's used in the rebasing process.
- **Timelocks and Circuit Breakers**: Introducing time delays and conditions that can halt operations if anomalous data is detected.

9.5 Proactive Monitoring and Contingencies

Proactive monitoring of the Oracle system's performance and regular audits of its security are essential to anticipate and address potential threats. Additionally, contingency plans, such as secondary oracles or manual override protocols, can ensure continuity of operations should the primary oracle system fail.

Using Bloomberg's pricing data through an Oracle system introduces a complex array of risks that must be carefully managed to maintain the integrity of STBT. While the risks cannot be eliminated, a combination of technological and procedural safeguards can significantly mitigate the potential for adverse outcomes, thereby ensuring the reliability and stability of STBT as a backing asset for the USDV stablecoin.

10 Proof of Reserves and Third-Party Auditor Framework and Risk

The transparency and trust in the Short-term Treasury Bill Token (STBT) are significantly bolstered by the Proof of Reserves (PoR) system and the role of third-party auditors. These components are fundamental in affirming the veracity of the assets backing the STBT, which is critical for its integrity and the confidence of its stakeholders.

10.1 Proof of Reserves (PoR)

The PoR is a mechanism that provides a public attestation to the actual holdings backing the STBT. It allows for verification that the underlying U.S. Treasury Bills adequately collateralize the number of tokens in circulation and reverse repurchase agreements. The PoR mechanism addresses the need for transparency in asset-backed tokens and is essential for maintaining the market's trust.

10.2 Third-Party Auditors

Third-party auditors play a vital role in independently verifying the STBT's reserve holdings. They scrutinize the PoR statements and conduct regular audits to ensure that the reported values are accurate and that the reserves are in place. This independent verification process prevents discrepancies or misrepresentations of the STBT's backing assets.

10.3 Verification Risk

The accuracy of the PoR is contingent on the precision of the data provided and the integrity of the verification process. There is a risk that the PoR could be compromised if the underlying data or the verification process is compromised.

10.4 Timeliness of Information

The value of the PoR and audits is highly dependent on their timeliness, as delays in updating the PoR or conducting audits can lead to discrepancies between the reported reserves and the actual holdings, especially in volatile markets.

10.5 Mitigation Measures

To mitigate these risks, STBT management must ensure the use of reliable data sources for PoR, engage reputable and independent auditors, maintain up-to-date and secure operational systems, and manage sensitive information dissemination carefully. Regular reviews of the PoR and audit processes are also essential to adapt to changing market conditions and regulatory requirements.

11 Depeg Risk

Depeg risk refers to the potential for a stablecoin or asset-backed token to diverge from its intended price peg. For the STBT, which is designed to maintain a stable value through its

backing by short-term U.S. Treasury bills and reverse repurchase agreements, depeg risk can arise from various market conditions and operational challenges.

11.1 Depeg Scenarios

The following scenarios can lead to a depeg of the STBT from its NAV:

- **Abrupt Withdrawals**: Large, sudden redemptions by STBT holders could require liquidating underlying assets at unfavorable prices, potentially leading to a depeg.
- **Operational Delays**: Delays in the rebasing mechanism due to operational issues could prevent timely adjustments of the STBT supply, causing a temporary depeg.
- **Underlying Asset Volatility**: Significant fluctuations in the value of the U.S. Treasury bills or the conditions of reverse repurchase agreements could lead to mismatches in the NAV, resulting in a depeg.
- **Smart Contract Failures**: Malfunctions or bugs in the smart contracts governing STBT could interfere with accurate pricing, leading to a depeg.

11.2 Mitigating Depeg Risk

To mitigate depeg risks, STBT management must implement strategies such as:

- **Liquidity Reserves**: Maintaining a reserve of highly liquid assets to manage large redemptions without impacting the underlying asset prices.
- **Rebase Optimization**: Ensuring the rebasing mechanism is responsive and efficient in adjusting the supply of STBT in alignment with its NAV.
- **Market Monitoring**: Continuously monitoring market conditions to anticipate and react to liquidity changes.
- **Smart Contract Auditing**: Regularly audit and test smart contracts' bugs or failures that could lead to depegging.

12 Redemption Risk in STBT and USDV Ecosystem

Redemption risk is a significant consideration in the stability and operation of financial assets like Short-term Treasury Bill Tokens (STBT) and USDV (a stablecoin backed by STBT). This risk becomes particularly pertinent in scenarios with a mass attempt to redeem these tokens simultaneously, potentially leading to a liquidity crisis. The primary concerns in such scenarios are the operational capacity to process high volumes of redemptions and the impact on the market value of the underlying assets during large-scale liquidations. The timelines for minting and redeeming STBT and USDV can range from a few minutes to several days, depending on various factors, including market conditions and operational efficiency.

12.1 Contextualization Within the U.S. Treasury Bill Market

When examining the scale of STBT operations within the broader U.S. Treasury Bill market, it's important to note the following:

- **U.S. Treasury Bill Market Size**: Historically, the U.S. Treasury Bill market has been one of the world's largest and most liquid financial markets, with over several trillion dollars markets.
- **STBT Market Scale**: Compared to the overall Treasury Bill market, the STBT market is much smaller. This relative size difference is crucial because it implies that even sizable redemption activities within the STBT market are unlikely to significantly impact the liquidity or pricing of the broader T-bill market.
- **Operational Competency as the Primary Concern**: Given the liquidity and vastness of the T-bill market, the real risk in the context of STBT and USDV is tied to the operational efficiency of the managing entities. The ability to process redemptions smoothly and maintain the integrity of the rebasing mechanism is vital.

12.2 Implications for USDV

- **Risk Transfer to USDV**: Considering that USDV is backed by STBT, the aforementioned risks and market dynamics directly impact USDV. Therefore, operational risks in STBT management translate into risks for USDV holders.
- **Contextualizing USDV Risks**: While the underlying asset (STBT) benefits from the liquidity and stability of the U.S. Treasury market, USDV's risk profile is also shaped by the operational and systemic efficiencies of the STBT management system.
- **Recommendations for USDV Integration**: For potential partners considering integrating USDV, viewing these risks through the lens of USDV's unique relationship with STBT is recommended. Partners should be cognizant of the operational and systemic risks while also considering the robust backing of USDV by one of the world's most liquid markets.

While the redemption risk in STBT and its impact on USDV is valid, it should be contextualized within the larger framework of the highly liquid U.S. Treasury Bill market. The primary risk factor shifts from market liquidity to operational competency in managing the STBT and, by extension, the USDV. Understanding this relationship and the operational dynamics at play for potential partners and users is crucial for informed decision-making regarding the integration and use of USDV.

13 Financial Risk Assessment

The financial risk assessment of the Short-term Treasury Bill Token (STBT) encompasses a range of risks that could impact its performance, stability, and the trust of its stakeholders. This assessment includes credit, liquidity, market, interest rate, and counterparty risks, each of which is critical to understand for anyone involved with STBT.

13.1 Credit Risk

Credit risk refers to the possibility that a borrower will default on their contractual obligations, impacting the lender's financial position. For STBT, credit risk is relatively low given its backing by U.S. Treasury bills, which are considered among the safest assets due to the creditworthiness of the U.S. government. However, the token may still face credit risk from the counterparties in reverse repurchase agreements. To manage this risk, STBT must carefully evaluate the creditworthiness of its counterparties and diversify its reverse repo agreements across reputable institutions.

13.2 Liquidity Risk

The portfolio composition of the Short-term Treasury Bill Token (STBT) is a critical factor in its operational stability and its function as the backing asset for the USDV stablecoin. Understanding the liquidity and duration of the portfolio is essential for assessing STBT's risk and return profile.

13.3 Portfolio Composition

STBT's collateral predominantly comprises a mix of short-term U.S. Treasury bills and reverse repurchase agreements. The treasury bills eligible as collateral have maturities of six months or less, aligning with the strategy to limit exposure to interest rate fluctuations and maintain the portfolio's short-term nature. This structure offers exposure to short-term U.S. interest rates while minimizing duration risk. The reverse repurchase agreements, which are short-term (typically overnight) instruments, are considered low-risk and use treasury bills as their underlying collateral. Currently, STBT's collateral is split approximately 90% in reverse repos and 10% in T-bills, reflecting a strategic preference for short-duration assets given the yield curve's current configuration and the project's early-stage status.

13.4 Duration Risk

Duration risk is managed by maintaining the portfolio's target duration and selecting underlying assets. The majority allocation to overnight reverse repo agreements ensures that the portfolio is not overly exposed to interest rate movements, which is a significant consideration for the stability and predictability of the returns for STBT holders and, by extension, the USDV stablecoin. Additionally, Matrixdock releases daily proof-of-reserve statements delineating the distribution between T-bills and reverse repo assets, providing transparency and building trust in the STBT's portfolio composition.

13.5 Liquidity

Liquidity in the portfolio is maintained by keeping the duration target relatively short, currently at around 5.5 days. This low-duration portfolio ensures the assets are highly liquid, which is crucial for meeting redemption demands. The T-bills are constantly rolled to keep the portfolio duration at this target length. T-bills must be sold before maturity to honor redemption requests if a substantial redemption demand arises. This sale before maturity could potentially result in a lower execution price for the T-bills, but the likelihood of such a scenario is mitigated by the portfolio's high liquidity and short duration.

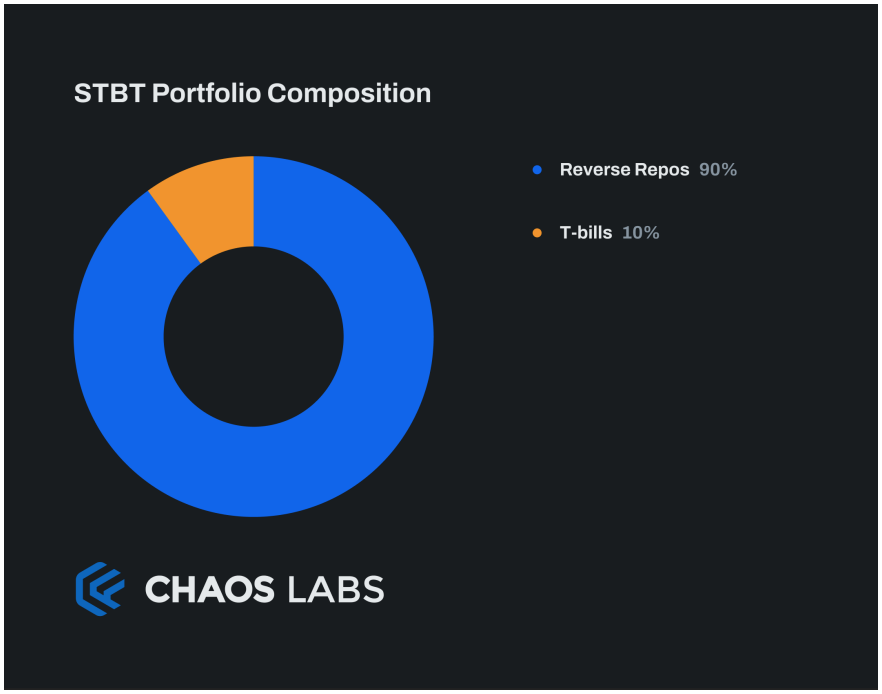


Figure 3.8

13.6 Market Risk

Market risk, or systematic risk, involves changes in market conditions that can affect the value of STBT, such as economic downturns or shifts in investor sentiment. STBT's market risk is inherently low due to the stable nature of its underlying assets. Nonetheless, adverse market movements, regulatory changes, or geopolitical events could impact the broader financial market and affect STBT's stability indirectly.

13.7 Interest Rate Risk

Interest rate risk is the risk that changes in interest rates will affect the value of financial assets. For STBT, this risk is associated with the possibility that fluctuating interest rates could impact the yield of the underlying U.S. Treasury bills and reverse repurchase agreements. Since STBT holds short-term instruments, the interest rate risk is minimized, but management must monitor the interest rate environment closely to anticipate and respond to potential changes.

13.8 Counterparty Risk

Counterparty risk is the risk that the other party in an agreement will default on their obligations. In the context of STBT, this risk is present in reverse repurchase agreements, where the counterparty may fail to fulfill its contractual obligation to repurchase the securities. To address counterparty risk, STBT must conduct thorough due diligence on its counterparties and may require collateral or other risk mitigation measures to secure the transactions.

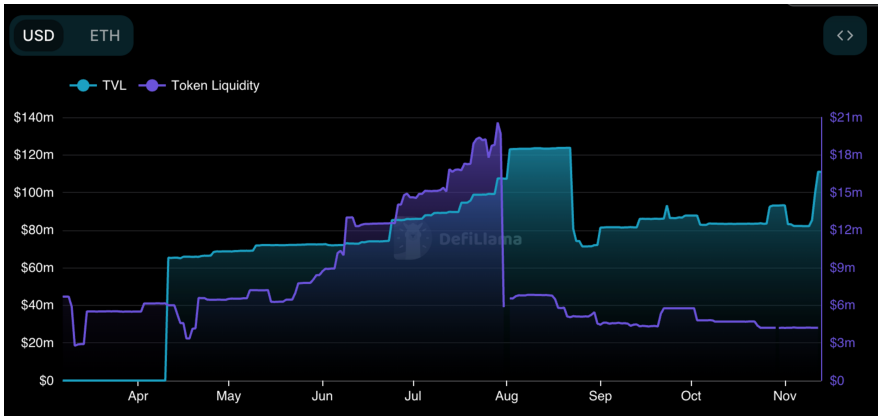


Figure 3.9: Overall liquidity for STBT since August is around $4M-$7M with market cap ranging between $80M-$100M. Below is a comparison of market depth between STBT, crvUSD, and LUSD with a market cap of $150M-$210M.

14 Centralization Risks

Centralization risk in the context of the Short-term Treasury Bill Token (STBT) pertains to the potential vulnerabilities and limitations arising from a concentration of control or influence within certain aspects of the token's ecosystem. This risk can manifest in various forms and have significant implications for the economic stability, security, and trustworthiness of the STBT.

14.1 Centralization Factors

Centralization factors refer to elements within the STBT's structure and operations that may lead to a concentration of power or dependency. These can include the reliance on a single entity for management decisions, such as Matrixdock's role in the operational management of STBT, or a dependency on a limited number of financial institutions serving as custodians or pricing providers. Such centralization can create points of vulnerability where the failure of a single entity or a small group could have outsized effects on the entire STBT system.

14.2 Economic Factors

The economic implications of centralization risk involve the potential for market manipulation, where a centralized authority could influence pricing or liquidity to its advantage. For STBT, economic centralization could also emerge from the concentration of token ownership, where major holders could impact the token's secondary market price through large-scale trades. Additionally, reliance on a single pricing source or a limited range of instruments for determining the NAV could lead to inaccuracies in valuation or hamper the token's ability to rebase effectively.

14.3 Security Factors

From a security standpoint, centralization can increase the risk of targeted attacks, such as hacking or social engineering efforts aimed at specific individuals or entities with control

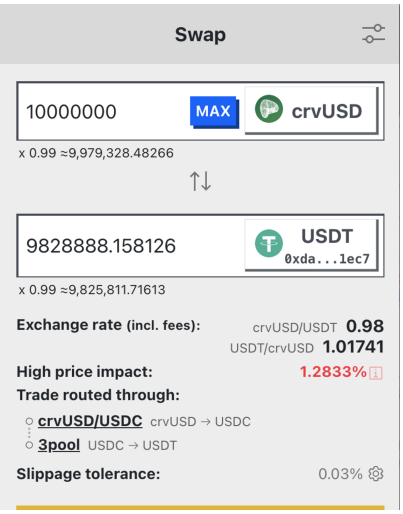


Figure 3.10: Liquidity for the crvUSD/USDT pair on Curve.

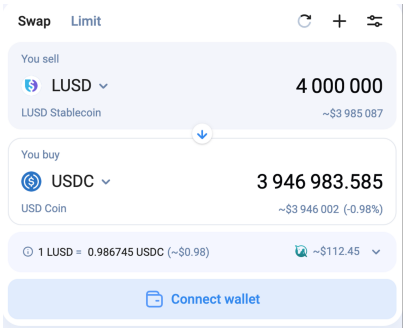


Figure 3.11: LUSD/USDC Liquidity as a reference.

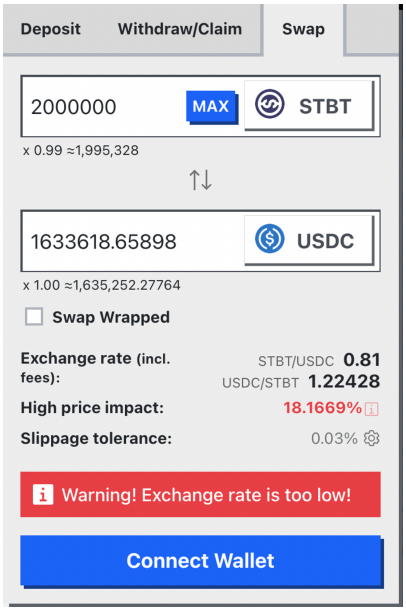


Figure 3.12: STBT/USDC Curve Depth

over the STBT's operational processes. Centralized decision-making and control mechanisms may also lead to less transparency, reducing the community's ability to identify or respond to potential threats. Moreover, centralized databases and infrastructure present attractive targets for malicious actors, and their compromise could lead to a loss of funds or disruption in STBT's operations.

STBT's governance and operations could incorporate decentralized mechanisms, such as distributed decision-making processes, reliance on multiple pricing sources, and diversifying custodial and operational entities to mitigate centralization risk. By spreading control and influence across a broader spectrum, STBT can enhance its resilience against centralization-related risks.

15 Operational Risk Assessment

Operational risk assessment for the Short-term Treasury Bill Token (STBT) encompasses evaluating the potential for loss resulting from inadequate or failed internal processes, people, systems, or external events. This assessment includes smart contract risks, the implementation of timelock mechanisms, custodial risks, transaction processing risks, and system and technology risks, which are essential to understand and mitigate in the daily operation of STBT.

15.1 Custodial Risks

Custodial risks refer to the potential loss of assets held by a third party or custodian. These risks can manifest as the result of internal malfeasance, external breaches, or insolvency of the custodian. Ensuring that STBT's custodians are reputable, insured, and compliant with stringent security practices is vital to minimizing custodial risks. Additionally, using

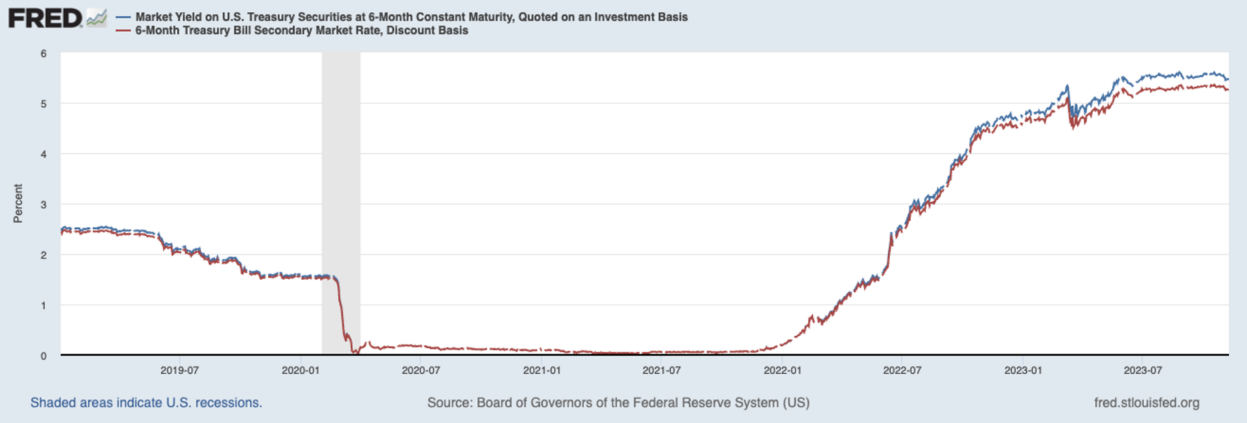


Figure 3.13: 6-Month T-Bills interest rates (blue) compared with 6-Month T-Bills Secondary Market Rate, Discount Basis. The Secondary Market Rate indicates the discount at which secondary market buyers are willing to buy T-Bills below their face value. Until mid-2022, the discount rate rarely exceeded 5bp, and over the past few months, given the short-term interest rate expectations, discount rates have gone up as high as 27bp.

multisignature wallets and regular reconciliation of holdings with public proof of reserves can further mitigate these risks.

15.2 Transaction Processing Risks

Transaction processing risks are associated with the execution of STBT transactions, including the minting, rebasing, and redemption processes. Operational errors, software malfunctions, or delays can lead to transaction failures or incorrect execution, affecting the token's reliability and user trust. Effective transaction monitoring systems, redundancy mechanisms, and rapid incident response protocols are essential to manage these risks.

Figure 3.14: Daily price chart of STBT in Curve from August '23 until November '23 exhibiting maximum intra-day volatility of 9.7%.

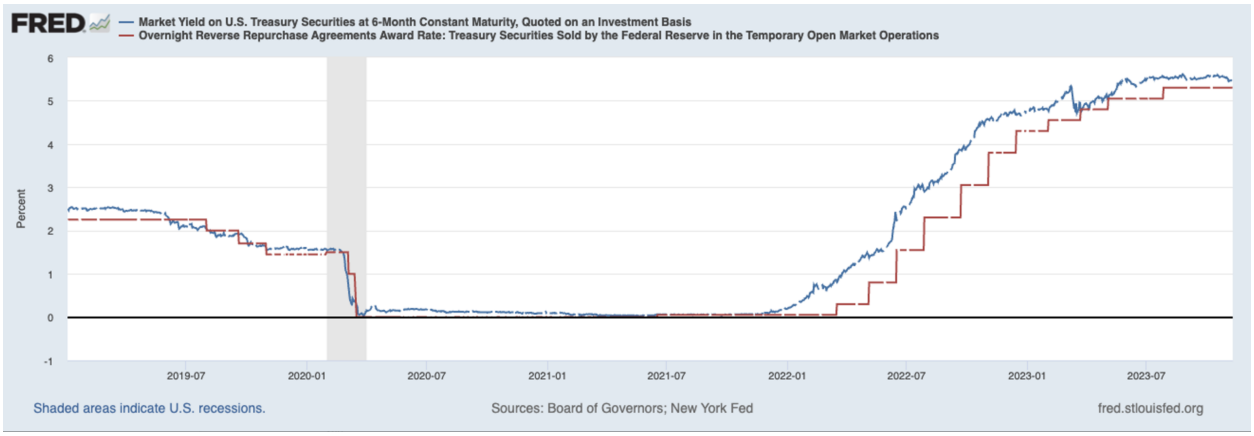


Figure 3.15: Source: Monetary Policy, Heritage.org

Chapter 4

USDV Risk Vectors

1 Overview

As we conclude our pre-launch risk assessment for USDV, we reflect upon the various pillars that constitute its foundational and operational framework. The innovative design of USDV, underpinned by the stability of the Short-term Treasury Bill Token (STBT), the precision of the ColorTrace algorithm, and the adaptability of its native on-chain fungibility token (OFT) system, positions it as a noteworthy entrant into the stablecoin arena.

The core of USDV's proposition lies in its aspiration to maintain a steadfast peg to the US dollar while navigating the complex currents of DeFi applications. A stablecoin's risk profile is intricately tied to market capitalization, peg stability, widespread usage, and influence over secondary market prices. These elements are indicators of the stablecoin's health and acceptance and its resilience against market volatility and systemic shocks.

In decentralized finance's dynamic and ever-evolving landscape, the true test of USDV's design and risk mitigation strategies will unfold in the live environment. Within the crucible of real-world application, the most critical risk vectors—such as liquidity depth, market cap scalability, user adoption, and peg adherence—will reveal their long-term implications.

Given this context, our stark and foremost recommendation is the vigilant and continuous monitoring of USDV's organic growth and demand across the various DeFi protocols. Real-time monitoring tools and responsive protocols must be in place to detect, analyze, and address issues as they arise. This proactive stance on surveillance will be crucial in managing and adapting to the risks inherent in the operation of a stablecoin.

As we look towards the official launch of USDV, we underscore the necessity of an agile, informed, and responsive approach to its stewardship. The anticipation of its performance in the DeFi ecosystem is tinged with both optimism for its potential and cognizance of the challenges it may encounter. Through the lens of cautious and meticulous oversight, USDV can aspire not only to endure but thrive.

1.1 Protocol Architecture

The USDV stablecoin protocol represents a pioneering approach in digital currency, primarily due to its unique integration of several innovative components. This protocol architecture is built upon the foundational pillars of the Short-term Treasury Bill Token (STBT) backing, the Color Tracing algorithm, and its native on-chain fungibility token (OFT) mechanism.

1.2 Pillars of the USDV Protocol

STBT Backing

USDV is intrinsically linked to the value of STBTs, backed by short-term U.S. Treasury bills and reverse repurchase agreements. This backing provides a reliable and stable underpinning for the USDV, assuring users of the intrinsic value and redeemability of the stablecoin.

ColorTrace Algorithm

A distinctive feature of USDV is the Color Tracing algorithm, which allows tracking and attributing demand generated by different applications within the USDV ecosystem. This mechanism is crucial for ensuring that contributors to the network are fairly rewarded for the demand they generate, fostering an equitable and transparent system.

Native OFT

USDV's architecture includes a native OFT, which enhances its utility across multiple chains. This interoperability is designed to cater to the expansive nature of decentralized finance, allowing USDV to operate seamlessly across various blockchain networks.

Vault Mechanism

The protocol incorporates a vault system where STBTs are held to back the issuance of USDV. This system is crucial for the minting and redemption processes that ensure the peg of USDV to the US dollar.

Minting and Redemption Processes

The deposit of STBTs collateralizes the minting of USDV tokens into the vault, while the redemption process allows users to convert USDV back into STBTs, maintaining the currency's stability and liquidity.

Yield Generation

USDV is designed to offer yield opportunities to verified minters generated from the underlying STBT assets. This aspect aims to incentivize holding USDV over other stablecoins that might not offer similar returns.

Regulatory Compliance

The protocol architecture is developed with a strong emphasis on compliance with existing financial regulations, ensuring the longevity and legal integrity of the USDV.

2 Risk Surfaces

2.1 Smart Contract Risk

Like any blockchain-based system, vulnerabilities in smart contract code could be exploited, leading to loss of funds or disruptions in the stablecoin's operations. As noted earlier, USDV

has been audited by reputable smart contract auditing firms.

2.2 Liquidity Risk

Maintaining sufficient liquidity to redeem USDV is vital. Market conditions could affect the liquidity of the underlying STBTs, thereby impacting USDV.

2.3 Regulatory Risk

Changes in regulatory landscapes could pose a risk to the operation and acceptability of USDV, mainly as it involves yield generation and cross-chain functionalities.

2.4 Depegging Risk

Although USDV is designed to be stable, external market forces or operational inefficiencies could temporarily cause it to lose its peg to the US dollar.

2.5 ColorTrace Complexity

While innovative, the sophisticated ColorTrace algorithm introduces complexity that could lead to attribution errors or inefficiencies in the system.

2.6 Centralization Risk

The reliance on a limited number of entities for operational decisions or custody of assets introduces centralization risk, which could lead to points of failure or manipulation.

3 USDV Minting and Redemption

The process of minting and redemption are crucial for the operation and stability of USDV, a stablecoin backed by Short-term Treasury Bill Tokens (STBT). These mechanisms ensure that the supply of USDV is aligned with the backing assets' value and that users can convert their tokens back to those assets or a stable value reference like the US dollar.

3.1 Minting Mechanism

3.2 Mechanism Description

USDV is minted through a smart contract when an equivalent value of STBT is locked in the USDV vault. Strict protocols govern the minting process to ensure that each new USDV token is fully backed, maintaining a 1:1 peg to the US dollar.

3.3 Risks

- **Over-collateralization**: Minting more USDV than the STBT backing can dilute the value and affect the stablecoin's peg to the dollar.
- **Smart Contract Vulnerability**: Flaws in the minting smart contract can be exploited, potentially allowing the creation of USDV without proper collateralization.

- **Regulatory Compliance**: The process must adhere to regulatory standards, and any oversight could result in legal repercussions affecting the minting operations.

3.4 Mitigation

- Implementing rigorous auditing and testing procedures for smart contracts.
- Maintaining strict collateralization monitoring and ratios.
- Ensuring regulatory compliance through continuous legal review and adaptation.

4 Redemption Mechanism

4.1 Mechanism Description

Redemption allows USDV holders to convert their tokens back into STBT. The user typically initiates this process, with the corresponding USDV tokens being burned or removed from circulation.

4.2 Risks

- **Price Impact**: Large-scale redemptions could impact the price of STBT in the open market, especially if the market depth is inadequate.
- **Operational Delays**: Delays in processing redemption requests can undermine confidence in USDV's stability and reliability.

4.3 Mitigation

- Establishing a robust liquidity management strategy, including reserve buffers.
- Staggering redemptions or employing mechanisms to reduce immediate market impact.
- Optimizing operational procedures to handle redemption requests promptly.

The minting and redemption processes of USDV are integral to its function as a stablecoin. While these mechanisms are designed with safety and stability, they inherently carry risks, particularly concerning managing the collateralized assets and the smart contract's execution. By addressing these risks through preventive measures and responsive strategies, the integrity and trustworthiness of USDV can be upheld.

5 STBT Analysis

The STBT (Short-term Treasury Bill Token) Risk Assessment summarizes the risks associated with STBT as a yield-generating, stable digital asset backed by U.S. Treasury bills and reverse repurchase agreements. The assessment covers various risk categories, including operational, market, credit, liquidity, counterparty risks, and specific mechanisms and strategies to mitigate those risks.

Here are the key points from the risk assessment summarization:

5.1 Operational Risks

These encompass the potential for loss due to failures in internal processes, people, or systems or from external events. Risks such as smart contract vulnerabilities, timelock mechanisms, custodial risks, transaction processing errors, and system and technology failures are analyzed with proposed mitigation strategies, including regular audits, multi-signature controls, and robust security measures.

5.2 Market Risks

These relate to changes in market conditions that could impact the value of STBT. Market volatility, economic downturns, and shifts in investor sentiment are considered. Diversification and maintaining a reserve fund are key strategies for mitigation.

5.3 Credit Risks

Given STBT's backing by U.S. Treasury bills, the credit risk is generally low but still present due to its involvement in reverse repurchase agreements. Mitigation involves careful counterparty creditworthiness assessments and diversification of reverse repo agreements.

5.4 Liquidity Risks

The potential inability to meet redemption requests without significant price impact is addressed by maintaining a highly liquid reserve and implementing staged redemption processes.

5.5 Interest Rate Risks

These are minimized due to the short-term nature of the underlying assets. However, management must closely monitor interest rate environments to anticipate and respond to changes.

5.6 Counterparty Risks

Risks from counterparties failing to meet their obligations in reverse repurchase agreements are mitigated through due diligence and requiring collateral where necessary.

5.7 Centralization Risks

Dependence on a single entity or a small number of entities for decision-making or operational management could introduce vulnerabilities. Decentralizing control and ensuring checks and balances are recommended mitigation approaches.

5.8 Depegging Risks

The risk of STBT's value deviating from its peg due to market liquidity fluctuations or operational issues is mitigated by maintaining a collateralization ratio and rebasing mechanisms.

The risk assessment concludes that while STBT presents a novel and promising financial instrument within the DeFi space, it is not without risks. The assessment recommends ongoing monitoring, regular updates to risk mitigation strategies, and transparency to maintain the trust and stability of the STBT. It's important to note that this summarization is based on the information provided and the typical content of a risk assessment document. An in-depth STBT Risk Assessment Document analysis would be necessary for a precise and detailed conclusion.

6 ColorTrace Algorithm

The ColorTrace algorithm presents a novel solution to the fungible token coloring problem, enabling the attribution of tokens to their respective minters across a multi-chain environment. The essence of the ColorTrace algorithm lies in its ability to maintain a global invariant, termed the delta-zero invariant, which assures that the net error across all domains within the network remains nullified.

At the core, ColorTrace introduces the concepts of $localMint$ and $delta\delta$. The $localMint$ for a given color represents the count of tokens on a blockchain that are accounted for in the vault, whereas $delta\delta$ signifies the discrepancy between $localMint$ and the actual circulation of tokens. The algorithm operates by ensuring that the sum of $localMint$ across all blockchains for any color remains equal to the mint of that color in the vault, thus allowing for the tracking of global demand and fair yield distribution.

ColorTrace employs two primary layers within its operational paradigm: the **coloring** and **synchronization layers**. The coloring layer is responsible for the assignment and reassignment of colors to tokens, enforcing transactions to be monochromatic, thereby simplifying the storage complexity to $O(1)$. The synchronization layer addresses the divergence created by the coloring layer through cross-chain messaging, ensuring that the global state remains consistent.

6.1 Attack Vectors on the Algorithm

The sophistication of ColorTrace does not render it impervious to potential exploit vectors. Below, we review two such vectors.

6.2 Flash Reminting

The "flash reminting" attack vector in the context of digital assets, particularly those like USDV or similar stablecoins, is a type of exploit that leverages the speed and mechanics of blockchain technology to gain undue advantages, typically in the form of disproportionate yields or profits.

How Flash Reminting Works

- **Utilization of Flash Loans**: An attacker initiates a flash loan, a large amount of capital borrowed and repaid within the same transaction block on the blockchain.
- **Rapid Minting and Reminting**: The attacker uses this capital to mint many tokens, like USDV, which may have a rebasing or yield-generating mechanism.

- **Exploitation of Yield Mechanisms**: The attacker can exploit the yield mechanisms by quickly minting and then reminting (or converting) these tokens. For instance, they might receive yield distributions or benefits disproportionate to their long-term investment in the token.
- **Repayment of Flash Loan**: Before the transaction block closes, the attacker repays the flash loan, often keeping any yields or profits generated from this rapid minting and reminting process.

Why It's Problematic

- **Unfair Gains**: This attack allows someone to reap benefits without a genuine, sustained investment, undermining the fairness of the yield distribution system.
- **Market Manipulation**: Such activities can distort token valuations and yields, impacting genuine investors and the overall market stability.
- **Resource Strain**: Flash reminting can strain the system resources, potentially leading to network congestion and increased transaction fees for other users.

Flash Remint Mitigations Implemented

- **Timelock Mechanisms**: Timelocks have been implemented, preventing immediate reminting, thus negating the benefits of a flash loan in this context.
- **Fee Structures**: Imposing fees on minting and reminting transactions can make flash reminting financially unviable. These will be modified continuously as a function of market demand and user behavior and serve as an additional lever to deter potential malicious actors.

6.3 Fugitive Deficit Attack

The "Fugitive Deficit Attack" is a potential exploit that targets the system's accounting mechanisms to evade the negative consequences of allowing the reminting of tokens colored by an entity.

Mechanism of a Fugitive Deficit Attack

- **Mempool Observation**: The malicious entity observes the mempool to identify transactions that attempt to remint tokens with the malicious entity's deficit as the target.
- **Synchronization Exploitation**: The attacker strategically synchronizes their transactions, front-running the remint transaction to remove these tokens.

Why It's Problematic

- **System Exploitation**: This attack manipulates the intended functioning of the token ecosystem, leading to unfair value distributions.
- **Burden on Honest Users**: Other users not part of the attack may unfairly lose yields.

- **Market Manipulation**: Such activities can create artificial market movements and undermine the token's trust.

Mitigation Strategies

- **Threshold control mechanism**: temporarily restricting the movement of specific-colored deficits or restricting the routing of deficit.

Chapter 5

Conclusions and Recommendations

1 Key Themes and Learnings

The comprehensive analysis of USDV, a stablecoin backed by the Short-term Treasury Bill Token (STBT), reveals a sophisticated and well-structured asset. Key themes include:

- **Robust Backing**: USDV's backing by STBT, which in turn is secured by U.S. Treasury bills, provides a strong foundation of stability and low risk.
- **Innovative On-Chain Attribution**: Implementing the color tracking algorithm to solve the fungible token coloring problem is a novel approach, enhancing transparency and fairness in yield distribution.
- **Best Practice Adherence**: The frameworks and structures employed for custodianship and daily attestations align with current best practices in the financial markets.
- **Audit and Verification**: The ColorTrace algorithm and operational processes have undergone audits by reputable smart contract audit firms, ensuring reliability and security.

1.1 Identified Risk Vectors

- **Operational and Regulatory Risks**: Operational efficiency and adherence to evolving regulatory standards remain crucial for USDV's stability.
- **Dependence on U.S. Government Securities**: While the risk is low, relying on the U.S. government's credibility and stability in honoring bonds is a fundamental dependency.
- **Secondary Market Pricing and Liquidity Risks**: As a new entrant in the market, USDV's liquidity and pricing in secondary markets are yet to be tested and observed.
- **Utilizing CPA Audit Reports**: We note that the current procedure involves The Network Firm performing daily assessments and verifications based on information shared by STBT's custodian. While this process provides a level of oversight, for enhanced assurance and to align with best practices in financial reporting, we recommend upgrading these daily reports to CPA-audited Daily Audit Reports. This enhancement would bolster the credibility and reliability of the reported information.

1.2 Integration Recommendations for Potential Partner Protocols

- **Initial Onboarding**: Given USDV's novel structure and promising backing, initial integration into partner protocols should be approached with caution, balancing enthusiasm with prudence.
- **Scaling with Demand**: Increase exposure progressively in alignment with observed organic growth, demand, and emerging use cases.
- **Money Market Considerations**: Money market configurations for USDV should reflect market demand and liquidity, ensuring stability.
- **Yield Generation**: For platforms (verified minters) considering USDV for margin while generating yield, a gradual approach is advised, monitoring its performance and stability.

1.3 Ongoing Monitoring and Real-Time Risk Management

- **Continuous Observation**: Monitoring user behavior, market acceptance, and demand patterns post-launch will be crucial in evaluating USDV's performance and stability.
- **Implementation of Risk Monitoring Systems**: Integrating real-time risk monitoring and anomaly detection systems is strongly recommended to add a layer of risk mitigation and security.
- **Comfort in Onboarding**: Chaos Labs, in its capacity as an evaluator, would feel more comfortable endorsing the onboarding of USDV to potential partners once these additional risk management systems are in place, ensuring a comprehensive approach to risk mitigation.

1.4 Final Recommendation

The conclusion of our assessment positions USDV as a low-risk and promising stablecoin option for verified minters, particularly suitable for cautious initial integration into isolated markets. This recommendation, however, is contingent on the implementation of real-time monitoring and sophisticated risk management systems, which are crucial for a fully confident and secure onboarding process.

We propose a cautious, data-informed strategy for integrating USDV, one that closely aligns with its natural growth and the demands of the market. This approach not only ensures a measured expansion but also aligns with risk mitigation principles.

Additionally, the assurance and confidence in USDV would be further enhanced by the implementation of daily CPA Audit Attestations on STBT, conducted by a selected third-party auditor. Such a practice would elevate the level of financial transparency and reliability, contributing significantly to stakeholder confidence.

It is also important to recognize that the current Proof of Reserve (PoR) asset attestation methodology employed by STBT is still regarded as best-in-class, particularly in the absence of established industry-wide standards. This methodology, while robust, would benefit from the added layer of security and credibility that daily CPA audits can provide, reinforcing USDV's position in the market as a stable and trustworthy digital asset.

Chapter 6

Helpful References and Resources

1 Resources

We express sincere thanks to the authors and creators of the various resources and references that have been instrumental in the development of this report. Your insightful audits, detailed documentation, and valuable materials, though created independently, have collectively formed a bedrock of knowledge that has greatly enhanced our work. We link to them here for the convenience of the reader.

- USDV Documentation
- STBT Documentation
- STBT Whitepaper
- STBT Statements
- Zellic USDV Audit
- Llama STBT Risk Report
- Ottersec USDV Audit

Appendix A

About Chaos Labs

Chaos Labs, an industry leader in the financial blockchain sphere, specializes in rigorous Risk and Economic Audits for decentralized finance (DeFi) applications. Specializing in blockchain applications, our company offers a cloud-based platform that develops risk management solutions and provides economic security tools for DeFi protocols utilizing crypto-native and real-world tokenized assets.

The Chaos Labs team exhibits exceptional talent and represents diverse expertise, encompassing esteemed researchers, engineers, and security professionals. Chaos Labs has garnered its experience and skills from renowned organizations, including Google, Meta, Goldman Sachs, Instagram, Apple, Amazon, and Microsoft. Additionally, the team boasts members who have served in esteemed cyber-intelligence and security military units, further contributing to their unparalleled capabilities.

Our platform utilizes Agent-Based Monte Carlo Simulations to stress test DeFi protocols under a wide range of adverse and volatile market conditions. These simulations form a crucial part of our Risk and Economic Audits, enabling us to meticulously evaluate the resilience and stability of these protocols against potential financial risks and economic regime shifts. Through our partnerships with top DeFi protocols, Chaos Labs is committed to innovating solutions that significantly enhance the efficiency and economic robustness of DeFi marketplaces. We aim to shape a more secure, transparent, and efficient DeFi ecosystem underpinned by our expertise in mitigating risks and fortifying economic sustainability.

You can explore our past and ongoing projects for customers like Aave, GMX, Benqi, dYdX, Uniswap, Maker, and more in the Research and Blog sections of our website.