

The Hidden Plumbing of Stablecoins

Financial and Technological Risks in the
GENIUS Act Era

The Hidden Plumbing of Stablecoins: Financial and Technological Risks in the GENIUS Act Era

Daniel J. Aronoff* F. Christopher Calabia[†] Anders Brownworth* Ashwanth Samuel*
Neha Narula*

Abstract

U.S. dollar stablecoins are increasingly used as payment and settlement instruments beyond cryptocurrency markets. With the enactment of the GENIUS Act in 2025, the United States established the first comprehensive federal framework governing their issuance, backing, and supervision. This paper evaluates the financial, technological, and regulatory risks that may arise as GENIUS-compliant stablecoins scale into mainstream use. We show that maintaining par-value redemption may depend not only on backing-asset quality, but also on the functioning of Treasury and repo markets, the balance-sheet capacity of broker-dealers, and the operational reliability of blockchain-based transaction rails. Even conservatively backed stablecoins can face stress from redemption surges, market-intermediation bottlenecks, or technological disruptions. We argue that durable stability will likely require an integrated approach spanning financial-market infrastructure, prudential regulation, and software governance. While grounded in U.S. law, the analysis identifies principles that are relevant for regulators in other jurisdictions developing stablecoin regimes.

1 Introduction

U.S. dollar stablecoins—digital tokens designed to maintain parity with the U.S. dollar and to circulate on blockchains—have rapidly grown in scale and policy relevance. They are widely used as settlement instruments across cryptocurrency markets and increasingly appear in emerging payment applications outside of the crypto ecosystem. This expansion, and forecasts of future potential, have prompted regulators to consider how instruments that resemble money in function, but not in institutional form, should be governed.

With the passage of the GENIUS Act in 2025, the United States established the first comprehensive federal framework governing the issuance, backing, and supervision of dollar-denominated stablecoins. The Act focuses on strengthening the quality of stablecoin issuer backing assets, improving transparency, and clarifying supervisory authority, with the goal of enabling the benefits of programmable, dollar-linked payment instruments while limiting obvious financial and operational risks. While the Act substantially improves reserve quality and disclosure, it implicitly treats stablecoin stability as a balance-sheet problem, resolvable

*MIT

[†]Bank of England. Contributions reflect work completed largely while at MIT, prior to the Bank of England. The opinions expressed in the paper are the authors' own and do not represent, and should not be reported as representing, the views of the Bank of England or any of its policy committees.

through conservative asset holdings and supervision. But a stablecoin’s ability to trade at par under stress depends not only on its asset quality, but on the functioning of redemption mechanisms, markets, and operational infrastructure. The GENIUS framework leaves these stress-contingent dynamics largely unspecified. This means that stablecoins deemed “safe” could still experience instability when market liquidity, dealer balance-sheet capacity, or technical systems are strained.

This paper addresses these gaps by analyzing the financial, technological, and regulatory risks most likely to arise under stress as stablecoins scale in volume and are integrated more deeply into the broader financial system. Our work is intended as a policy-oriented risk analysis rather than an assessment of stablecoins’ desirability, long-run adoption prospects, or impact on global currency arrangements. Instead, we ask more fundamental questions: *If stablecoins become widely used as payment and settlement instruments, what might go wrong with the guarantee of par? What regulatory, institutional, operational, or technical mechanisms might help prevent destabilizing outcomes?*

To answer these questions, we analyze vulnerabilities that emerge at three interconnected layers of stablecoin architecture: the financial structure of the issuer’s balance sheet and the markets that facilitate the trade of backing assets, the technology that governs stablecoin token creation and transfer, and the regulatory framework that constrains (or fails to constrain) issuer behavior. Importantly, these layers interact in ways that can amplify stress. We show that ensuring a stablecoin can be redeemed for a dollar, also known as *par-value exchange*, depends not only on the quality of assets backing the stablecoin, but also on the functioning of Treasury and repo markets, the balance-sheet capacity of broker-dealers, and the operational reliability of the blockchains that enact token transfer. Even when stablecoin issuers hold conservative portfolios, frictions in market intermediation or surges in redemption demand could, under stress, test the robustness of par-value exchange. In addition, technological risks—arising from smart contract logic, blockchain consensus mechanisms, bridges, oracles, and governance design—may impair transferability or redemption in some circumstances, potentially affecting confidence, even when reserves remain intact.

Although the analysis is grounded in U.S. law and institutions, the mechanisms we identify are relevant for regulators outside the United States. Stablecoins circulate globally, and many of the financial and technological channels we examine—market-intermediated liquidation, dealer balance-sheet constraints, and blockchain operational risk—are not jurisdiction-specific. As other authorities design or refine stablecoin regimes, the interactions documented here may inform supervisory and policy choices.

We preview three high-level conclusions. First, asset quality alone is insufficient to guarantee par-value stability if redemption depends on intermediated markets subject to capacity constraints. Second, blockchain-based rails introduce operational risks that differ in kind from those faced by traditional payment systems and can interact with and amplify financial stress. Third, the GENIUS framework provides a strong foundation but leaves unresolved policy dilemmas concerning liquidity support, capital buffers, and redemption design that will shape outcomes in stress scenarios.

1.1 Roadmap

Section 2 describes key elements of stablecoins under GENIUS and situates stablecoins in the hierarchy of money. We clarify the distinction between solvency and liquidity and describe the mechanics of minting new stablecoins and redemption. We then turn to the question of whether stablecoins can reliably maintain par value in times of stress. In Section 3 we explain how to consider the insolvency risk of stablecoin issuers given interest rate movements. In Section 4 we compare a stablecoin issuer's balance-sheet structure with those of commercial banks and money market funds, emphasizing differences in liability redeemability, asset liquidity, balance-sheet discretion, capitalization, and liquidity-management tools. These contrasts clarify why stablecoin issuers may face greater challenges in maintaining par despite holding high-quality assets.

In Section 5 we turn to risks arising when issuers liquidate Treasuries to process redemptions. We examine dealer-balance-sheet bottlenecks and we review past episodes of fragility in Treasury and repo markets. These factors imply price risk to stablecoin issuers attempting to liquidate Treasuries to meet redemption runs, and could influence the broader Treasury markets. The section culminates in the outline of a policy dilemma: granting stablecoin issuers access to the Federal Reserve's balance sheet could alleviate liquidity bottlenecks and reduce risk, but doing so carries significant complications for monetary policy transmission and could potentially disintermediate banks.

Stablecoins run on permissionless blockchains, which are relatively novel infrastructure in the financial system and are not yet systemically important. Section 6 turns to the technical and operational risks that arise from these systems; even if a stablecoin issuer has the financial capacity to maintain par-value, the technological infrastructure determines whether users can actually access, transfer, and redeem their coins in practice. We discuss risks arising from smart-contract bugs, key custody, bridges, oracles, underlying blockchain consensus security, quantum computers, network congestion, and governance designs. Although some risks are in the control of the stablecoin issuer, many are not. We present a risk framework and suggestions for best practices to mitigate risks. In Section 7 we explore additional channels through which technical failures can propagate into financial instability.

Section 8 evaluates the scope and limits of the GENIUS Act as a foundation for stablecoin oversight, considering both the statutory mechanisms that promote stability and, as of yet, unresolved questions. We assess how well the Act addresses liquidity risks, redemption mechanics, market-structure vulnerabilities, and the technical fragilities we identify, and we surface areas where prudential tools, supervisory guidance, or new interagency coordination may be needed. In doing so, we situate stablecoin regulation within the broader U.S. monetary and financial architecture, clarifying how GENIUS both aligns with and departs from existing frameworks governing banks, money market funds, and other issuers of demandable liabilities. Section 9 concludes.

2 Key elements of stablecoins

A stablecoin is a blockchain-based asset whose issuer pledges to maintain parity with a central bank-issued currency. In this section, we first outline salient provisions of the GENIUS Act that delimit the backing asset allocations of stablecoin issuers. We next place GENIUS-compliant stablecoins in the monetary complex and explain the difference between issuer solvency and liquidity. After that discussion, we explain the process of redeeming and minting stablecoins—which we will draw on in our discussion of redemption risks in Section 5.

2.1 GENIUS provisions

The key provisions regarding par-value and backing asset requirements in the GENIUS Act are as follows.

Sec.2(22)(A)(iii)

(I) [The stablecoin issuer] is obligated to convert, redeem, or repurchase for a fixed amount of monetary value, not including a digital asset denominated in a fixed amount of monetary value; and

(II) represents that such issuer will maintain, or create the reasonable expectation that it will maintain, a stable value relative to the value of a fixed amount of monetary value;

Sec.4(a)(1)(A) [A stablecoin issuer shall] maintain identifiable reserves backing the outstanding payment stablecoins of the permitted payment stablecoin issuer on an at least 1 to 1 basis, with reserves comprising...

(i) United States coins and currency...

(ii) ...demand deposits [of banks]...

(iii) Treasury bills, notes or bonds-...

(iv)[Treasury] reverse repurchase agreements...

There are three key financial requirements under GENIUS: (i) A stablecoin issuer must redeem its stablecoin into bank deposits or cash at par with eligible counterparties, i.e., \$1 of stablecoin can be exchanged for \$1 of cash or bank deposits, (ii) A stablecoin issuer is required to maintain an expectation that its stablecoin will trade at par-value with the dollar and (iii) the stablecoin issuer must secure the value of its stablecoin liabilities with backing assets composed of cash, bank deposits, or US Treasury liabilities (“Treasuries”).¹ We explore how the allowed scope of backing assets, (iii), affects the ability to maintain par-value, (i) and (ii).

¹Treasuries can include direct ownership, repos and futures.

Other stablecoin attributes There are some types of stablecoins that are explicitly excluded under GENIUS. For example, algorithmic stablecoins that rely on arbitrage mechanisms between cryptocurrencies, rather than backing assets, to maintain par-value are excluded. Terra-Luna, which collapsed in 2022, is the most prominent member of this group (Liu et al., 2023).² In addition, some properties appear to be left to the discretion of stablecoin issuers, such as the protocol chosen by the stablecoin issuer for redeeming stablecoins. At one end, every stablecoin owner can redeem directly with the stablecoin issuer. At the other end, the stablecoin issuer designates a small number intermediaries to act as market-makers in purchasing stablecoins and then either warehousing and re-selling at a later date, or redeeming with the stablecoin issuer. Currently, the predominant stablecoin issuers (Circle and Tether) use intermediaries.

2.2 The position of stablecoins in the hierarchy of money

To facilitate our discussion of stablecoin financial risks, we describe the position occupied by stablecoins in the hierarchy of the U.S. monetary system. The hierarchy is composed of interlocking sectoral balance-sheets in which the liabilities of one sector are securities of, and settlement currency for, the adjacent sector lower down the hierarchy (Mehrling, 2013). At the top of the hierarchy is the central bank (the Federal Reserve), with assets comprised primarily of U.S. government debt, and liabilities comprised of reserves and cash.

Next in the hierarchy are banks, with assets comprised of central bank liabilities—reserves and cash—alongside loans. Inter-bank payments are settled by transferring reserves. Banks issue deposit liabilities, which they guarantee to convert into cash at par, i.e., \$1 of a bank deposit is exchangeable for a \$1 cash liability of the Fed. Bank deposits (and cash) are assets of, and money for, the non-financial sector, which in turn issues securities. These are liabilities whereby the issuer promises to pay holders scheduled amounts of bank deposits at future dates. What ties the hierarchy together is the ability to convert the liabilities at one level, e.g., bank deposits, into liabilities of the next level up, e.g., cash at short notice at par (i.e., on demand). Notably, it is not the actual volume of conversions that enforce par, but the *option to convert*.³

Stablecoins are monetary liabilities that lie lower in the hierarchy than deposits and cash, because redemption normally settles in commercial bank deposits and can require market intermediation to transform securities into deposits. This placement, however, is not automatic. It is a function of institutional design: if stablecoin issuers can hold central bank reserves as a backing asset and can settle redemptions and payments in central bank money without relying on sponsoring commercial banks, stablecoins can approach the same position in the hierarchy as commercial bank money.⁴ By contrast, when redemption settlement relies on

²GENIUS (Sec.14) mandates a study of algorithmic stablecoins for potential future regulatory approval.

³“Private bank deposits remain at par with currency because of the guaranteed option of conversion into central bank money. It is the existence of the option, not the frequency of its use, that keeps the system anchored” (Goodhart, 1988). We can add that convertibility in the other direction, from cash into bank deposits, is also required.

⁴The Bank of England has proposed a design that allows stablecoin issuers to hold central bank reserves and borrow from the central bank (Bank of England, 2025a). In Section 5.5 we discuss tradeoffs, in terms of cost and other tradeoffs, this arrangement implies.

commercial bank deposits and dealer-intermediated liquidation of securities, as is the case under GENIUS, stablecoins remain lower in the hierarchy even when the reserve portfolio is high quality. Figure 1 displays the position of GENIUS stablecoins in the hierarchy and outlines the redemption process.

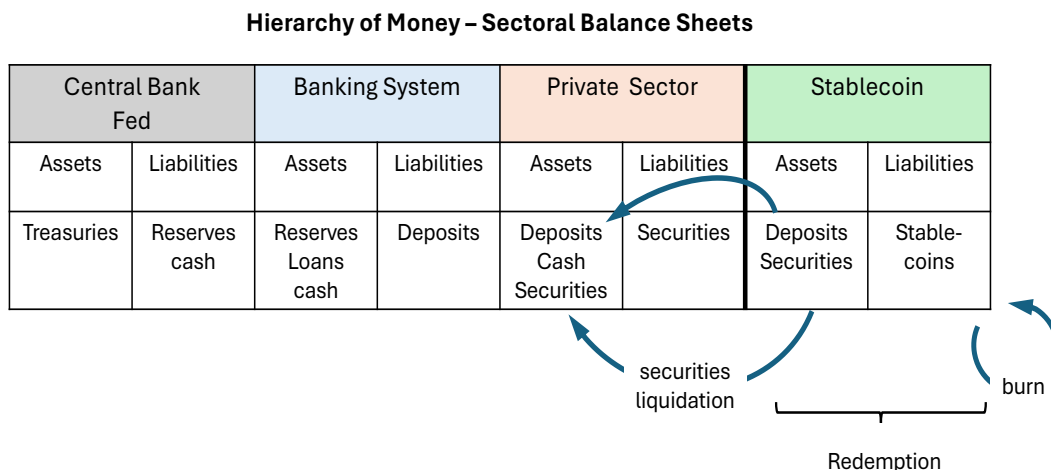


Figure 1: A securities-backed stablecoin is redeemed by liquidating securities to obtain bank deposits.

2.3 Liquidity and solvency

There are two key elements implicit in the definition of par-value exchange. One is *solvency*; the market value of backing assets must exceed stablecoin liabilities. The other is *liquidity*; the backing assets, to the extent they are composed of Treasury securities, must be sold in a timely manner to meet redemptions. Securities vary in terms of liquidity; a comparatively more liquid security is defined as “being more certainly realizable [into bank deposits or cash] at short notice without loss” (Keynes, 1930). The most liquid securities are Treasury bills, Treasury repos, and money market fund shares. Solvency is a necessary, but not sufficient, condition to maintain par-value exchange: execution requires liquidity. Most of the time, redemptions are processed without delay at par-value. In a stress event where redemption demand spikes, Treasury market infrastructure—broker-dealer market-making capacity, trading software systems, etc.—can become overwhelmed by the flood of selling orders, leading to price collapse and/or delayed transaction processing.⁵ It is at those critical moments of market stress that par-value is tested. At such times, the ability to maintain par-value exchange is determined by the liquidity of the securities that the stablecoin issuer must sell to redeem its stablecoins.

This motivates a conceptual partition of GENIUS-authorized stablecoins into those backed by bank deposits and those backed by securities. The “convenience yield” of bank deposits—arising from their superior payment and liquidity services—causes them to yield less than other securities (Mishkin, 2019; Holmström and Tirole, 1998; Vayanos and Vila, 2021). The convenience yield for a stablecoin issuer arises from the

⁵In Section 5.1 we review recent episodes of stress in the US Treasury market.

stablecoin redemption process. The yield spread between Treasury securities and bank deposits provides incentive for the stablecoin issuer to hold the former as its primary backing asset, which implies a tradeoff of yield for liquidity. The stablecoin issuer can immediately redeem with a bank deposit it holds as a backing asset. By contrast, when the backing asset is a security, the stablecoin issuer has the added step of liquidating the security into a bank deposit to redeem. Selling the Treasury adds a layer of risk and delay. Bank deposits can be transferred instantaneously with FedNow, whereas Treasury transactions require one day ($T+1$) to settle. Two things to note about this partition are the following:

- A stablecoin issuer can operate on both sides of the partition if it holds bank deposits and securities, as most do. When it redeems using pre-existing deposits, the stablecoins are bank deposit-linked. When it liquidates a security to obtain a bank deposit, the stablecoins are securities-backed.
- The distinction is based on liquidity, not solvency. A bank deposit is not solvent, and may not be honored, if its bank is insolvent. This risk was underscored in 2023 when Circle, the issuer of stablecoin USDC, was temporarily unable to transfer its \$3.3 bn of uninsured deposits held at Silicon Valley Bank (SVB), which had become insolvent.⁶

2.4 Stablecoin redemption and minting mechanics

As discussed in Section 2.2, par-value is enforced by the option to convert the lower form of money, in this case stablecoins, into the higher form of money, in this case bank deposits, and back again.⁷ Here we briefly describe the mechanics of how minting and redemption work assuming the stablecoin issuer is not simply using bank deposits to back its tokens. Note that, perhaps counterintuitively, the process of redeeming and minting stablecoins does not directly involve a change in the overall volume of bank deposits.⁸

Redemption. Figure 2 depicts the redemption process when the stablecoin issuer holds securities as the backing asset and liquidates Treasuries (denoted T). The sequential order is as follows.

1. The redeemer sends the stablecoin with value $\$x$ to the stablecoin issuer in a blockchain-based smart contract. The stablecoin issuer then removes it from circulation.
2. The stablecoin issuer sells Treasuries. This results in the buyer of the Treasuries sending (i.e., subtracting) $\$x$ from its bank deposit account in return for receipt of T Treasuries. The buyer's bank transfers $\$x$ of reserves to the stablecoin issuer's bank in exchange for the transfer of bank deposit liability. The buyer will typically be a broker-dealer in the secondary market for Treasuries.

⁶In the event, Circle's bank deposit account was effectively bailed out by the Fed
<https://www.financemagnates.com/cryptocurrency/svb-crisis-circle-escapes-usdc-depeg-with-regulatory-assurance/>

⁷We use "minting" to denote the entry of stablecoins into circulation. This is a slight abuse of the term, since a stablecoin issuer, or its distributor, can retain minted stablecoins as reserves to meet future demand. This has been a common practice.

⁸We do not here explore the possibility of second-order effects on bank deposits such as changes in monetary policy prompted by growth of stablecoins that may cause the volume of reserves, and thereby deposits, to be altered.

3. The stablecoin issuer sends T to the buyer and receives an increase of $\$x$ in its bank deposit account. Thereupon, it sends $\$x$ to the redeemer's bank deposit account, which reduces its bank deposit account to the initial level. The stablecoin issuer's bank transfers $\$x$ of reserves to the redeemer's bank in exchange for the transfer of bank deposit liability.
4. The redeemer receives an increase of $\$x$ to her bank deposit account.

At the end of the redemption, the redeemer has exchanged a stablecoin for an equal value increase in her bank deposit account, and the stablecoin issuer has reduced its liabilities and assets each by $\$x$. Note, however, an orderly redemption requires that the Treasury can be sold “at short notice without loss” (which still requires $T+1$ to settle). In Section 5 we explore the viability of this assumption. Finally, note that redemption does not alter the volume of bank deposits. The value $\$x$ moves from the deposit account of the Treasury buyer to the redeemer's account (via the stablecoin issuers bank deposit account).⁹

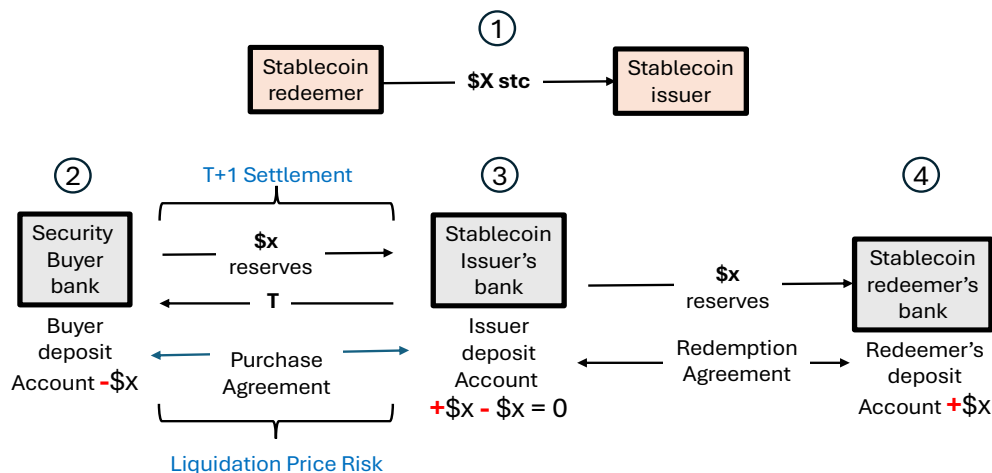


Figure 2: Redemption stablecoin payments flow

Minting. Figure 3 depicts the flow of central bank reserves and deposits that takes place when a new stablecoin is minted. The interpretation of the chart is similar to Figure 2. Moving from left to right, the buyer sends an $\$x$ deposit to the stablecoin issuer for the purchase. If the stablecoin issuer elects to hold a Treasury security, it sends the deposit to the seller of the Treasury security as payment for the security. The deposit value moves between accounts, but the net value is unchanged. As with redemptions, minting generates no change in bank deposits. The deposit value $\$x$ moves from the buyer's bank deposit account to the Treasury seller's account. At some point during this process, the stablecoin issuer issues a blockchain transaction to credit the buyer's account in a smart contract on a public blockchain.

⁹In the event the stablecoin issuer redeems with bank deposits it holds as a backing asset, Step 2 is eliminated and the transfer moves directly from the stablecoin issuers bank deposit to the redeemer's bank deposit.

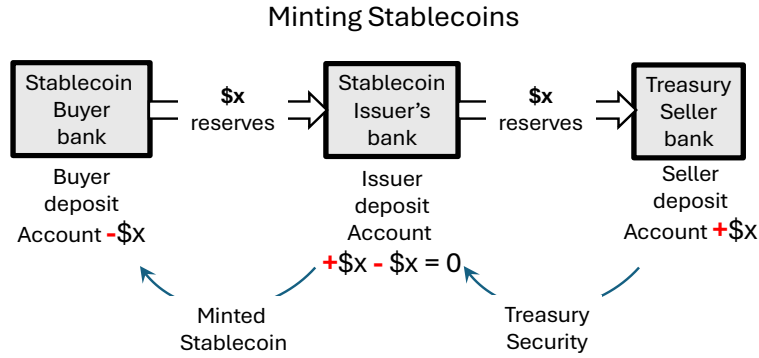


Figure 3: Minting stablecoin flow

Direct vs. indirect access to minting and redemption. At the present time, the two dominant stablecoin issuers, Circle and Tether, do not offer minting and redemption services to anyone. Instead, these services are limited to sets of intermediaries who in turn interact with stablecoin buyers and sellers on a secondary market (primarily cryptocurrency exchanges).¹⁰ Ma et al. 2025 present an interesting tradeoff between par and run-risk: With direct access, there is no incentive to trade in a secondary market for stablecoins because every owner has the option to redeem at par. However, this increases the incentive to redeem at times of market stress, thereby increasing run risk. On the other hand, indirect access induces a secondary market with prices that can deviate from par, but reduces the incentive to run precisely because par-value is not guaranteed, even to the early movers.

2.5 Challenge maintaining par-value without open market operations

As far as we know, today the largest stablecoin issuers do not engage in open market operations to maintain the exchange rate of their stablecoin tokens on secondary markets, like cryptocurrency exchanges. However, we note that depending on how strictly the par-value requirement of GENIUS (Sec 2(22)A(iii)) is interpreted and enforced, stablecoin issuers might need to exercise lesser or greater control over the volume of stablecoins in circulation.

A par-value requirement can be analyzed along two dimensions: the goal of the requirement and the methods to achieve the goal. *The goal* is to enable an owner of a stablecoin to redeem or sell her stablecoin for a fixed dollar amount. This can be interpreted in at least two ways. One way is to require that the stablecoin can be sold “on short notice without loss [i.e., at par]”. This is a rigorously fixed exchange rate. It can alternatively be interpreted as allowing the exchange value to fluctuate within defined bounds, above and below par-value. This is a corridor target.

The method to achieve the goal has to do with how the stablecoin issuer adjusts the supply of its stablecoins,

¹⁰Notably, the EU MiCA stablecoin regulations require direct access.

where the circulating supply of a stablecoin at a point in time is the difference between the cumulative quantity minted and redeemed by the stablecoin issuer. There are three ways in which a stablecoin issuer can intervene to alter supply:

1. Directly mint or redeem stablecoins based on requests from buyers and sellers at par-value (specified by MiCA)
2. Mint or redeem from intermediaries at par-value, who, in turn, buy or sell on secondary markets (how Circle and Tether currently operate)
3. Create new stablecoins and offer them for sale without an initiating request, or purchase stablecoins on secondary markets¹¹

We do not know the specific goal that will ultimately be enforced (a rigorously fixed exchange rate, a corridor target, or merely a best-effort attempt at par), or whether there will be directions on the use of methods. We can, however, comment on the difference in discretionary control that the stablecoin issuer will have under the three types of goals.

Rigorous fixed exchange rate. Under strict enforcement of par-value, the supply of stablecoins would be determined by the demand to acquire or to redeem stablecoins. The stablecoin issuer would passively adjust supply to these market forces (method 3). The reason is that, to maintain par at every moment in time, the stablecoin issuer would need to make a standing offer to redeem or purchase when the stablecoin is below target, to reduce supply to accommodate market demand to convert stablecoins into dollars, and mint when it is above target, to accommodate market demand to convert dollars into stablecoins. This places the stablecoin issuer in a position similar to a central bank that maintains a fixed exchange rate with an offshore currency. It is an axiom of monetary theory that the domestic money supply is endogenously determined by the requirement to maintain par when the central bank commits to a fixed exchange rate with another currency or asset (such as gold).¹²

Corridor around par-value. A corridor, which establishes a range of exchange values, would provide the stablecoin issuer discretionary control over the stablecoin supply inside the corridor. Here the stablecoin issuer can allow the exchange rate to drift above par without minting, or allow it drop below par without redeeming. Outside the corridor market forces will dictate the adjustments to supply the stablecoin issuer will need to effectuate, engaging in method 3.

No strict enforcement of par-value. In this case, GENIUS is interpreted to require stablecoin issuers

¹¹There are two circumstances where minting in response to a demand for stablecoins may not be feasible, even as the value of the stablecoin is above par. One is during a financial crisis where a contraction of credit limits the volume of stablecoins that arbitrageurs are able to purchase. The other is where the interest rate on bank deposits and Treasury securities drop below the level required for the stablecoin issuer to make a profit, for example if interest rates are negative. In that case, the stablecoin issuer will be reluctant to mint. These constitute—possibly irreducible—gaps in the ability of a stablecoin issuer to maintain par-value.

¹²“...under fixed exchange rates the central bank does not control the money supply since it must fix the exchange rate.” (Krugman et al. 2012).

to provide par-value exchange only with the set of intermediaries who have access to direct minting and redemption with the stablecoin issuer. Many stablecoin holders might experience a loss of par-value.

3 Insolvency risk

The GENIUS Act requires a stablecoin issuer to maintain backing assets at least equal in value to its stablecoin liabilities (Sec.4(a)(1)(A)).¹³ It is a knife-edge requirement. A stablecoin issuer that “just” meets the requirement at one moment will become insolvent the next moment if the market price of its backing assets falls by any amount. This is a nontrivial risk as Treasuries are subject to interest rate risk, i.e., their value moves inversely to their yields. In this section, we explain how the two dominant stablecoin issuers, Tether and Circle, have mitigated interest rate risk by allocating the majority of their backing asset into short duration securities. This minimizes interest rate risk and maximizes flexibility to liquidate securities to meet redemption demands. Equation 1 shows the progression of a stablecoin issuer’s backing assets value over time.¹⁴

$$A_{t+1} = A_t + \underbrace{r_{t,T}T_t + (T_{t+1} - T_t)}_{\substack{\text{interest} \quad \text{capital gain} \\ \text{Treasury securities}}} + \underbrace{r_{t,D}D_t + (D_{t+1} - D_t)}_{\substack{\text{interest} \quad \text{capital gain} \\ \text{bank deposits}}} \quad (1)$$

In Equation 1 time is partitioned into a sequence of periods denoted $t, t+1$ etc... A_i is the value of the stablecoin issuer’s backing assets at the beginning of period i ; T_i and D_i are the stablecoin issuer’s investment in Treasuries and bank deposits at the beginning of period i and $r_{i,T}$ and $r_{i,D}$ is the interest paid on Treasuries and bank deposits in period i , which is fixed at the beginning of period t . The *level* of interest rates earned on backing assets—so long as it exceeds the stablecoin issuer’s operating cost—adds to the value of backing assets. The primary source of insolvency risk is from a capital loss, i.e., $T_{t+1} < T_t$. Capital loss is caused by a decline in interest rates from the beginning of period t to the beginning of period $t+1$. In other words, capital loss is determined by *timepath* of interest rates on backing assets.¹⁵ GENIUS requires that a study of possible capital rules be undertaken but at present there is no mandate. In this case it is left to the stablecoin issuers to determine their own investment and retention policies.

¹³The GENIUS Act (Section 4.(4)(A)) directs certain regulatory agencies to issue capital and liquidity requirements for stablecoin issuers, which may, inter alia, mandate an increase in the 1:1 capital requirement. We do not here speculate on the content of future rules.

¹⁴GENIUS prohibits stablecoin issuers from paying interest on liabilities. This eliminates a source of solvency risk that is present in banks, who pay interest on deposits and other liabilities.

¹⁵Here we treat backing assets under GENIUS as “safe assets” and ignore default risk.

3.1 Backing asset allocations

The reported asset allocations of the two dominant stablecoin issuers, Circle and Tether, are concentrated in short duration securities, notably overnight reverse repos and Treasury bills.¹⁶ In terms of equation 1, the interval between t and $t + 1$ is short, which minimizes the risk of capital loss.

	Repo	Treasury bills	Bank deposits	Bitcoin	other
Circle	43	24	11		
Tether	21	113	6	10	18

Table 1: Backing Asset Allocations Circle and Tether Q3 2025 (in billions USD).¹⁷

3.2 Reverse-repos provide a capital cushion

Here we explain how reverse-repos provide the stablecoin issuer with maximal protection against capital loss. In a reverse-repo trade, the stablecoin issuer lends bank deposit money in the repo market and receives Treasuries in exchange, with an agreement to resell those Treasuries at a later date. A repo trade is composed of two contracts entered into at the same time. A contract for party A to purchase Treasuries from party B today (the “first-leg”), and a contract for party B to re-purchase the same type—CUSIP or general collateral—and volume of Treasuries from party A at a future date (the “second-leg”). Effectively, party A is making a collateralized loan to party B. GENIUS allows stablecoin issuers to hold reverse Treasury repos.

Typically, repo borrowers—the counterparties to stablecoin issuers in the repo trade—provide excess Treasury collateral, referred to as the “haircut”.¹⁸ The haircut provides the stablecoin issuer insurance against capital loss. The short time period of the overnight trade (24 hours), or the twice-daily re-margining that applies to longer duration repos, limits the size of tail—i.e., extremely large—capital loss. For a haircut of size H —meaning that the Treasuries held by the stablecoin issuer exceed the value of its first-leg purchase by H —the Treasury can be liquidated and the stablecoin issuer will receive back its purchase price for any decline in market price up to H . Figure 4 displays the effect of a haircut in a repo lending trade (it omits interest payments for simplicity). The vertical axis is the market price of Treasuries. The horizontal axis is time t .

It depicts a decline in value between the first-leg at time t and the second-leg at time $t + 1$, of Δ where the haircut H (i.e., the value of excess collateral) exceeds the price decline ($H > \Delta$). Without the excess collateral H , the value of the Treasuries would drop below the purchase price. This outcome would occur

¹⁶We do not address controversies surrounding the veracity of the reported asset positions.

¹⁷Figures rounded to the nearest billion USD. Circle source: Deloitte Independent Accountant’s Report, November 26, 2025. Tether source: BDO Independent Auditors’ Report, October 31, 2025. Note that Tether’s figures include non-US domiciled stablecoins, which lie outside the jurisdiction of GENIUS.

¹⁸For example, the standard haircut in the tri-party repo market is 2% (Paddrik et al., 2021). However, there may not be a haircut when the counterparties have another trade that offsets the risk of the repo trade (Hempel et al., 2023b).

if the stablecoin issuer purchased Treasuries in the secondary market. Treasury repos add two layers of protection. One layer is that the repo counterparty has a contractual obligation to repurchase at the second-leg, notwithstanding a decline in market price. The second layer is that the haircut adds excess collateral, which creates a cushion that enables the stablecoin issuer to liquidate, if necessary, and recover its first-leg purchase price, up to a decline of H .

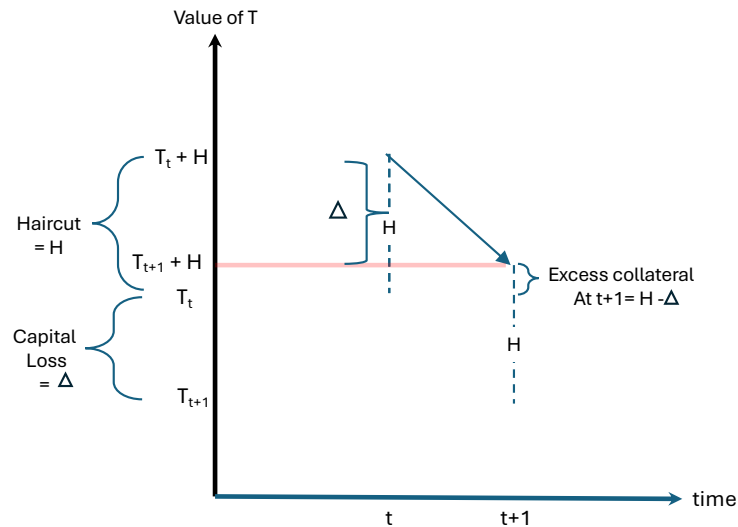


Figure 4: Repo Lending with Haircut

Observations We make three observations regarding the protection against capital loss provided by reverse repos.

1. The counterparty has a contractual obligation to repurchase the Treasury at the negotiated price, regardless of any decline in its market value.
2. If the stablecoin issuer's counterparty fails to repurchase, the stablecoin issuer can liquidate the Treasury in the secondary market and recover its first-leg purchase price, for any decline in market value of the Treasuries collateral up to the haircut.
3. The stablecoin issuer can mitigate its risk of capital loss by sequencing overnight repo trades—"rolling over." When Treasury yields are increasing (i.e., price is declining) the stablecoin issuer receives back its initial purchase price at the second-leg and re-lends (i.e., enters into a new reverse repo trade) its money at a higher interest rate the next period, and so on.

3.3 Summary

GENIUS does not (yet) promulgate a capital adequacy standard for stablecoin issuers. The two largest issuers have chosen to mitigate their insolvency risk by investing in short duration Treasury securities. Opinions may differ on whether that is an adequate cushion against capital loss. There are two paths forward concerning stablecoin issuer capital standards. One way is for regulators to establish capital adequacy rules that address the risk of insolvency (which we address in Section 4) and illiquidity (which we address in Section 5). The other way is to allow stablecoin issuers to choose their backing asset portfolios and compete for acceptance by the public, subject to the constraints in the extant legislation.

4 Building a resilient balance sheet

In the prior section, we explored how two stablecoin issuers sought to mitigate their exposure to interest rate risk so that their backing assets remain at least equal in value to their stablecoin liabilities and they can honor redemptions at par. Now we broaden our scope to consider how stablecoin issuers hedge against unexpected losses stemming from all risks, including operational and broader market rate risks. The design of a stablecoin issuer’s balance sheet differs markedly from the most familiar financial institutions that offer similar par-value promises, namely commercial banks and money market mutual funds (MMFs). Understanding the structural differences in balance sheet designs is critical for assessing the solvency, liquidity, and run risks associated with stablecoin issuers, even for those that are aligned with the GENIUS Act.

To keep the promise of par-value redemptions, stablecoin issuers must invest proceeds from coin sales in assets that preserve value and can be liquidated quickly at low cost. Under the GENIUS Act, licensed issuers are largely confined to cash (in U.S. dollars), bank deposits, and short-term U.S. Treasury-related securities (12 U.S.C. §§ 5901–5916, 2025a). These constraints are intended to limit credit risk in the reserve portfolio, but they do not eliminate exposure to interest-rate, operational, or broader market risks.¹⁹

To date, stablecoin issuers have generally not been subject to bank-like capital requirements. The GENIUS Act empowers regulators to issue capital and liquidity requirements that are “tailored to the business model and risk profile of permitted payment stablecoin issuers.” Regulators have not yet issued these requirements, but the law appears to restrict U.S. regulators from applying the minimum leverage and risk-weighted capital requirements that govern commercial banks under the “Collins Amendment” directly to stablecoin issuers (12 U.S.C. §§ 5901–5916, 2025b); see also (Sullivan & Cromwell LLP, 2025). A central question is therefore whether a portfolio of high-quality, rapidly turning over assets provides sufficient protection against losses from interest-rate, operational, and market risks. If not, explicit capital buffers or other financial resources may be needed to ensure that stablecoin issuers remain operational and honor par redemptions.

For stablecoin issuers, this analysis is complicated by their reliance on novel technologies. Disruptions in

¹⁹Liang (2025a) notes that the Act does not distinguish between holdings of insured versus uninsured deposits, the latter of which may increase an issuer’s exposure to run risk.

the underlying technology do not directly alter the market value of reserve assets such as U.S. Treasuries. Frictions or failures in the systems used to transfer those assets or convert them into cash could nonetheless undermine confidence in the stablecoin, depress its market price, and impair the issuer's ability to redeem at par. We discuss in detail these technological and operational risks in Section 6.

Prudent balance sheet design and management of reserve backing assets, liabilities to stablecoin owners, and the issuer's own funds are therefore necessary but not sufficient conditions for preserving the par-value exchange. We will draw on key risk measurement and mitigation practices that commercial banks and money market mutual funds or their regulators use and compare their balance sheets with those of stablecoin issuers to understand their respective risks.

4.1 Comparing stablecoin issuers to commercial banks

When a stablecoin issuer receives cash from coin buyers, it records the proceeds as liabilities and invests them in reserve assets. These assets are chosen for their perceived safety (asset quality) and their ability to be sold quickly for an amount at least equal to the requested redemption (liquidity). Under the GENIUS Act, the issuer retains the income on reserve assets and does not share it with stablecoin owners, much as in some traditional intermediation arrangements. This resemblance has led some commentators to view stablecoins as equivalent to bank deposits; see (Armstrong, 2025) in the Financial Times.

The parallel with banks is useful but incomplete. We highlight five characteristics that differentiate the liquidity and strength of stablecoin issuers' balance sheets from those of commercial banks (redeemability, liquidity of assets, control over balance sheet growth, access to public support, and capital cushions) and assess the implications for resilience and par-value redemption.

Redeemable liabilities. Stablecoin issuers are more exposed to bank-style runs because nearly all of their liabilities are redeemable on demand. Commercial banks, by contrast, fund themselves with a mix of demandable and non-demandable liabilities. In U.S. aggregate data for 2024, checking deposits (17%) and overnight repos and federal funds (10%) are payable on demand, while savings deposits (35%) are not (Board of Governors of the Federal Reserve System, 2024). By this simple metric, banks are more insulated from immediate withdrawals than stablecoin issuers.

Liquidity of assets. Commercial bank assets are much less liquid than the assets held in stablecoin reserve portfolios. Loans account for roughly half of bank assets and are neither payable on demand nor easily sold quickly without incurring losses. Stablecoin reserves, in contrast, typically consist of U.S. Treasury securities, repos, and bank deposits or cash. Treasury-related instruments and cash can usually be liquidated rapidly and at or near par, provided that Treasury markets remain orderly and stablecoin issuers retain access to them. This structure suggests that stablecoin issuers may be better positioned than banks to meet sudden surges in redemption requests, although this conclusion depends critically on the behavior of Treasury markets under stress, which we examine in Section 5.

Control over balance sheet growth. Commercial banks have more discretion over their balance sheet growth. They can choose whether to expand or contract loan portfolios, decide which borrowers to serve, and adjust the composition of assets and liabilities over time. Stablecoin issuers, in contrast, have limited control over the size of their balance sheets: to prevent their coins from trading above par, they must generally accommodate demand for new coins by accepting cash and expanding reserves. Their balance sheets will tend to expand when demand is high and contract when demand is low. The GENIUS Act restricts their investment choices largely to Treasury-related securities and deposits at commercial banks.

Access to public support. Commercial banks benefit from multiple forms of explicit and implicit public support. Eligible deposits are insured by the Federal Deposit Insurance Corporation (FDIC), for which banks pay a premium but in return obtain a strong guarantee that bolsters depositor confidence. Banks also have access to central bank liquidity through the Federal Reserve’s discount window and standing repo facilities, especially in times of stress. Under the GENIUS Act, licensed stablecoin issuers do not receive deposit insurance and currently lack routine access to such public backstops, leaving them more reliant on their own assets to meet unexpected losses or rapid redemption waves.²⁰

Capital and solvency. Banks and stablecoin issuers differ sharply in how they use capital to absorb losses. Bank capital consists of equity—funds raised through stock issuance or retained earnings—that stands junior to deposits and other liabilities. Accounting identities require assets to equal liabilities plus capital. A bank funded entirely by deposits with no capital buffer would become insolvent if any borrower unexpectedly defaulted on a loan. Sufficient capital therefore protects solvency and enhances resilience; see Farag et al. (2013) for a primer.

Capital requirements are set in part by regulation. The GENIUS Act establishes a Stablecoin Certification Review Committee (SCRC) comprising the federal banking regulators, chaired by the Secretary of the Treasury, to develop the regulatory framework for licensed issuers. The same agencies—the Federal Reserve, the Office of the Comptroller of the Currency (OCC), and the FDIC—set capital and liquidity standards for commercial banks, drawing on international guidance from the Basel Committee on Banking Supervision.

(Because issuers with less than \$10 billion in coins outstanding may opt for state-level regulation, the GENIUS Act requires the Secretary of the Treasury to “establish principles” for determining the equivalence of a state’s regulatory framework with the federal approach. See 12U.S.C.§5903(c)(1)–(2).)

The current global framework, Basel III, requires banks to maintain minimum capital ratios and robust liquidity buffers that reflect their risk profiles. We benchmark stablecoin issuers against one key element of this framework: the simple leverage ratio, defined as equity divided by total assets. This is the most basic Basel capital requirement and is the metric that U.S. regulators use as a trigger for “prompt corrective action” when banks become dangerously undercapitalized. Note that we are not arguing that it is appropriate

²⁰For comparison, the Bank of England’s November 2025 consultation paper (Bank of England, 2025b) proposes that systemic sterling-denominated stablecoin issuers hold 40% of reserve assets in non-remunerated central bank deposits and notes that the Bank is “considering providing access to a backstop lending facility for eligible, solvent, and viable systemic stablecoin issuers.”

for stablecoin issuers to meet commercial bank capital requirements; we find this exercise useful as a proxy for understanding a stablecoin issuer’s capacity to withstand unexpected losses due to stress.

Using public filings, we construct a simplified leverage ratio for five prominent stablecoin issuers over three to ten recent quarters, depending on data availability. Data limitations prevent us from applying more complex risk-weighted capital ratios or the Basel liquidity standards, so our analysis focuses on this single, foundational measure. For banks, higher leverage ratios indicate greater loss-absorbing capacity and better protection for depositors. For stablecoin issuers, the leverage ratio captures the degree to which outstanding coins are overcollateralized.

Let total assets equal the value of reserve assets and total liabilities equal the value of coins in circulation. Capital is then the difference between assets and coins, and the leverage ratio is calculated as follows:

$$\text{Leverage ratio} = \frac{\text{assets} - \text{stablecoins}}{\text{assets}}$$

We apply this measure to five issuers that disclose sufficient information to approximate total assets and liabilities. The period we study is transitional: the reserve backing asset portfolios largely predate the GENIUS Act, and several issuers hold a broader range of assets than the Act would permit, including corporate bonds, secured loans, and volatile cryptoassets such as Bitcoin. Three issuers—Circle, PayPal, and Paxos—report reserve backing assets consisting primarily of cash or deposits and Treasury-related securities, and thus appear closer to the GENIUS standard, though we cannot verify full compliance.

Under the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), U.S. commercial banks must maintain leverage ratios of at least 4% to be considered adequately capitalized and at least 5% to be considered “well capitalized.” Banks with leverage ratios below 4% are undercapitalized, below 3% significantly undercapitalized, and below 2% critically undercapitalized. Regulators are required to intervene and take “prompt corrective action” when banks fall below 4% leverage ratios and, for critically undercapitalized banks, to move expeditiously toward receivership. See (Federal Deposit Insurance Corporation, 2022) and (U.S. Government Accountability Office, 2024). Licensed stablecoin issuers currently operate without an analogous prompt-corrective-action regime.

Table 2 reports the leverage ratios we compute.

None of the three issuers whose reserves most closely resemble the GENIUS requirements—Circle, PayPal, and Paxos—would have been classified as adequately capitalized (under expectations for bank) over the period we study. Two would have been critically undercapitalized in every quarter for which data are available; the third moved from significantly to critically undercapitalized in the final two quarters.

In contrast, the issuers with riskier backing assets that are not GENIUS-aligned were better capitalized under the leverage ratio. Tether met the 4% minimum leverage requirement in five quarters and exceeded the 5% “well capitalized” threshold in two of those. However, these figures reflect reserve portfolios that included

Table 2: Leverage ratios (%). Sources: (Tether, 2025; Circle, 2025; Paxos, 2025a,b; Ripple, 2025), also see Appendix A for methodology.

Stablecoin	2023				2024				2025	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
Tether USDT	2.99%	3.81%	3.71%	5.61%	5.68%	4.50%	4.86%	4.93%	3.75%	3.36%
Circle USDC	0.16%	0.20%	0.21%	0.21%	0.16%	0.16%	0.18%	0.15%	0.04%	0.11%
PayPal PYUSD	–	–	2.14%	2.29%	2.26%	2.16%	2.11%	2.16%	0.27%	0.42%
Paxos USDP	0.00%	–	0.00%	–	–	0.61%	0.01%	0.11%	0.13%	0.03%
Ripple USD	–	–	–	–	–	–	–	7.21%	4.43%	3.40%

higher-risk assets such as corporate bonds and Bitcoin.²¹ The remaining issuer, Ripple, met the minimum requirement in two quarters and was well capitalized in one of them.

Absent other mitigating factors, most stablecoin issuers in our sample would have been subject to prompt corrective action and required to raise additional capital or face increasingly stringent supervisory intervention had they been regulated as banks. The three issuers with reserve backing assets most closely aligned with the GENIUS standards might at times even have been candidates for receivership under FDICIA-style rules. In contrast, the remaining two with seemingly riskier backing assets generated higher leverage ratios that sometimes approached or met commercial bank requirements for this simplest measure of capital, suggesting that their balance sheets may be more resilient.

Moreover, the dispersion of leverage ratios across all five issuers, ranging from near zero to just above 7%, suggests that issuers either place little weight on capital as a risk mitigant or lack consensus on what constitutes adequate solvency. Some issuers seek indirect protection by investing heavily in overnight reverse repos, where borrowers post excess collateral under Fixed Income Clearing Corporation rules, but it is unclear whether such excess collateral would be sufficient or available to absorb large unexpected losses. In addition, retained earnings may grow over a longer time frame than what we studied and add to the capital buffer, but the growth of that capital element depends on an issuer’s financial performance and decisions of its board and senior management.

Because the GENIUS Act appears to preclude applying commercial bank minimum leverage requirements directly to stablecoin issuers, policymakers may implicitly be relying on liquidity alone, rather than solvency, to ensure resilience. This makes robust liquidity-risk measurement and management crucial, which we address next.

²¹Please see Appendix A for a short discussion of the dependence of Tether’s leverage ratio on Bitcoin. Tether has recently announced plans to issue a new U.S. dollar-based stablecoin, USAT, that it intends to be GENIUS-compliant. (Tether, 2025)

4.2 Comparing stablecoin issuers to MMFs

The liquidity structure of stablecoin reserve portfolios resembles that of money market mutual funds (MMFs). MMFs lack deposit insurance but are subject to regulations that limit their investments to mitigate run risk. MMFs invest in short-term, low-risk debt securities and seek to offer investors a cash-like instrument. Before 2014, MMFs maintained a fixed net asset value (NAV) of \$1 per share and were said to “break the buck” when their NAV fell below \$1. A 2014 reform required a switch to floating NAVs for prime funds, liquidity fees, and redemption gates to increase transparency and reduce run incentives (U.S. Securities and Exchange Commission, [n. d.]).

Anadu et al. 2024 describe the close parallels between stablecoin issuers and MMFs: both raise funds by issuing liabilities payable on demand, and both aim to provide par-value redemption—MMFs in dollars, stablecoin issuers in dollars or dollar-linked tokens. One key difference is that, since December 2015, MMFs have been allowed to lend to the Fed via its Overnight Reverse Repurchase Agreement (ON RRP) facility.²² This provides MMFs with a backstop that guarantees repayment. In terms of the hierarchy of money in Figure 1, it effectively integrates government security MMFs into the same level as the banking system.

MMF regulation requires funds to hold a minimum volume of short-duration assets. The Securities and Exchange Commission (SEC) limits eligible reserve assets to U.S. dollar-denominated securities and constrains portfolio maturity by requiring a dollar-weighted average maturity (WAM) of no more than 60 days and a weighted average life (WAL) of no more than 120 days. At least 25% of assets must be held in instruments that mature within one business day (daily liquid assets) or five business days (weekly liquid assets). The referenced 2014 reform, which required MMFs to use a floating rate net asset value (“NAV”) for prime funds (which invest in commercial paper), triggered a massive exit of 70% from prime funds (approx. \$825bn), the majority of which shifted into fixed NAV government securities funds (Allen and Winters, 2020)²³. See Section 5.4 for a discussion of informationally insensitive assets applied to the Treasury markets.

We adapt the Daily Liquid Assets (DLA) and Weekly Liquid Assets (WLA) concepts to stablecoin issuers. Before the GENIUS Act, issuers varied widely in the detail and quality of their disclosures. Circle and Paxos provide granular audits and attestation reports, including CUSIP-level detail, which allow reasonably precise estimates of DLA and WLA shares. Tether, by contrast, discloses the composition of its USDT reserves but not maturities, making strict application of the framework impossible. For the issuers where we can approximate DLA and WLA, a clear pattern emerges: reserves have migrated toward highly liquid securities—U.S. Treasuries and overnight repos—leaving DLA and WLA well above the MMF thresholds. At least some issuers thus appear to be converging, intentionally or not, toward MMF-style reserve practices.

²²Prior to that date MMFs were eligible counterparties in limited amounts as part of a test program. See (Hempel et al., 2023a) for a discussion of the ON RRP.

²³Holmström (2015) describes a MMF with a fixed NAV as “informationally insensitive”. The 2014 shift of prime funds to floating NAV made them less money-like. This has been proposed as an explanation for the magnitude of withdrawals (Allen and Winters, 2020)

Not all issuers have followed this path. Some continue to hold assets with potentially higher price volatility, including corporate bonds, precious metals, and cryptocurrencies such as Bitcoin. Stablecoins backed by such portfolios may face a greater risk of “breaking the buck” if many stablecoin owners seek to redeem simultaneously.

The 2014 reforms required MMFs to impose liquidity fees and redemption gates during periods of market stress. These mechanisms were designed to slow withdrawals and reduce investors’ incentives to run preemptively. However, subsequent analysis by the Government Accountability Office (GAO) finds that these reforms did not prevent large-scale redemptions from MMFs during the COVID-19 pandemic. Indeed, investors may have accelerated withdrawals to avoid the possibility of future gates or fees (U.S. Government Accountability Office, 2023). Analogous tools, even if permitted for stablecoin issuers, would thus be unlikely to eliminate run risk.

4.3 Summary and implications

Comparative resilience of banks and MMFs. Taken together, the five balance sheet characteristics—the share of liabilities redeemable on demand, the liquidity of assets, control over balance sheet growth, access to public support, and capitalization—suggest that commercial banks enjoy a more resilient structure for maintaining par-value claims than do current stablecoin issuers. Banks limit the fraction of immediately redeemable liabilities, exercise greater control over balance sheet evolution, hold larger capital buffers, and benefit from deposit insurance and central bank backstops.

With regard to liquidity, MMFs have been specifically designed with guardrails to mitigate run-risk and over time some stablecoin issuers have developed reserves that tend to mimic MMF asset composition. Stablecoin issuers that mirror MMF asset portfolios likely have similar liquidity to MMFs, from purely an asset perspective; however, the GENIUS Act states that redemptions for stablecoin issuers must occur “without delay.” Although the effectiveness of redemption gates and liquidity fees have been mixed, stablecoin issuers lack access to similar tools to potentially slow down redemptions during runs.

Risks for stablecoin issuers. Stablecoin issuers typically invest in high-quality, liquid assets such as Treasury-related securities, but most of the issuers in our sample appear to have thin capital buffers by bank standards. The most GENIUS-aligned issuers had the weakest capitalization when measured using the leverage ratio, suggesting that their balance sheets are the most fragile. Our findings indicate that, in the face of large interest-rate, operational, or market shocks, many issuers could become insolvent, jeopardizing their ability to honor par redemptions. Moreover, if many issuers were forced to sell Treasury-related securities simultaneously, the resulting market impact could itself impair liquidity and valuations, a possibility we explore in Section 5.

Regulatory implications. Because the GENIUS Act does not appear to authorize the straightforward application of Basel-style capital requirements to preserve solvency, regulators will need to rely on other tools to

strengthen the resilience of stablecoin balance sheets. One natural candidate is a framework of explicit liquidity requirements, adapted to the structure of stablecoin issuers and informed by experience with MMFs.

5 Redemption risks due to Treasury market fragility

GENIUS limits stablecoin issuer asset allocation to bank deposits and Treasury securities. The latter requires a stablecoin issuer to liquidate Treasury securities to meet its redemption payment obligations. Though these are large, liquid markets, they have suffered disruption in the past. In this section we review two recent episodes of disruption of the Treasury markets that were associated with relatively small shocks to the demand for Treasuries. We explain how this fragility is amplified by the interaction of accounting rules and bank capital regulations, which limit the volume of repo trades a bank affiliate broker-dealer can intermediate, and a mal-distribution of central bank reserves that impedes the channeling of reserves to broker-dealers to meet an uptick in selling pressure. These factors create a two-way channel between Treasury market stress and redemption runs. In one direction a run to redeem that increases selling pressure – even by a modest amount – can disrupt the market. In the other direction, a modest disruption in pricing or processing of sales can trigger a run to redeem. We then argue that the Fed’s standing repo facility does not achieve the intended goal of alleviating the capacity constraint in the Treasury market. We discuss the effects of granting stablecoin issuers access to the Fed’s balance-sheet and point out a crucial policy dilemma: On the one hand, redemption risk can be mitigated by allowing stablecoin issuers to hold central bank reserves. On the other hand, granting stablecoin issuers access to the Fed’s balance sheet could alter the transmission of monetary policy and disintermediate banks.

5.1 Reliance on the Treasury markets

The largest markets for Treasury securities are (i) the secondary market for sale and purchase of Treasuries and (ii) the repo market.²⁴ The former has daily turnover of approximately \$900 billion (Liang, 2025b). The latter has average daily turnover of approximately \$12 trillion (Hempel et al., 2025). These are the two largest volume financial markets in the world. By conventional metrics used in finance they are the most liquid markets and by historical price variability they are the most stable. Currently, stablecoin issuer backing assets are concentrated in short term Treasury securities, which provide a cushion against capital loss (Section 3). Nevertheless, there is a fault line running through the Treasury market that makes it fragile in the face of a spike in selling pressure, such as can occur during a run to redeem a stablecoin.

A redemption that is met by liquidating treasuries triggers a two-way interaction with the market that can amplify stress. In one direction, an uptick in redemption demand can push broker-dealers to the limit of their capacity to purchase Treasuries. In the opposite direction, when broker-dealers have reached that limit—possibly for reasons unrelated to redemptions—the disruption to processing redemptions can cause a run to

²⁴Original issue auctions of Treasuries is a third market that can only be accessed by Primary Dealers and individual investors.

redeem. We examine those interactions and show that the underlying source of redemption risk arises from the fact that Treasury markets are intermediated by broker-dealers with limited capacity to process trades, and in fact a reduced incentive to process trades, in times of market stress.

5.2 Recent disruptions in Treasury markets

Table 3 summarizes two recent instances of disruption in the Treasury markets; one in the repo market and one in the secondary market.

Event	Date / window	Yield dislocation (Treasury / repo)	Trading volume effect (Treasury / repo)
September 2019 repo spike	16–18 Sept. 2019	SOFR jumped from about 2.43% on Sept. 16 to 5.25% on Sept. 17, with some intraday transactions reportedly near 10%; the spread of SOFR over the top of the federal funds target range exceeded 300 basis points (Anbil et al., 2020), (Paddrik et al., 2023)).	SOFR transaction volume on Sept. 17 reached about \$1.18 trillion, around \$20 billion higher than the previous day (a low single-digit percent increase), indicating that the episode was driven more by an extreme funding-rate dislocation than by an unusually large surge in underlying transaction volume (Anbil et al., 2020)
March 2020 “dash for cash” in Treasuries	Late Feb.–late Mar. 2020 (esp. week ending 4 Mar.)	The 10-year Treasury yield fell to an intraday low near 0.5% and then backed up by roughly 60+ basis points over a few days; off-the-run issues underperformed on-the-run benchmarks and bid–ask spreads widened by an order of magnitude, reflecting severe dysfunction in Treasury market liquidity. (Fleming and Ruela, 2020), (Haddad et al., 2021))	Overall Treasury market trading volume reached record highs: in the week ending March 4, average daily volume exceeded \$1 trillion—roughly twice its post-crisis average—implying on the order of a 100% increase in cash-market turnover relative to normal conditions; primary-dealer volumes in mid-March were similarly elevated (Fleming and Ruela, 2020), (Duffie et al., 2021)).

Table 3: Yield dislocations and associated trading volume increases in U.S. Treasury and Treasury repo markets during two recent stress events: the September 2019 repo spike and the March 2020 “dash for cash”.

The yield spike in September 2019 was not associated with any appreciable change in transaction volume. March 2020 is more relevant for our analysis, since it was characterized by a run to exchange Treasuries for cash. In that event trading volume increased by an estimated \$500 billion.²⁵ Note, however, that this

²⁵Secondary Treasuries sales increased from a weekly average of \$2.5–\$3 trillion for four weeks prior to the event, to \$4.9 trillion

represents *gross* volume. An important fact is that the secondary Treasury market is intermediated by broker-dealers, who stand between the ultimate seller and buyer of Treasuries.²⁶ Figure 5 displays a chain of trades in the Treasury market with ultimate seller (or repo borrower) and buyer (or repo lender) at each end and two broker-dealers intermediating in the middle, which represents the average length of trading chain in the two Treasury markets.²⁷ The liquidation starts with the sale of Treasuries to broker-dealer #1. The Treasuries are either absorbed by a broker-dealer, or are passed on to an ultimate buyer on the right.

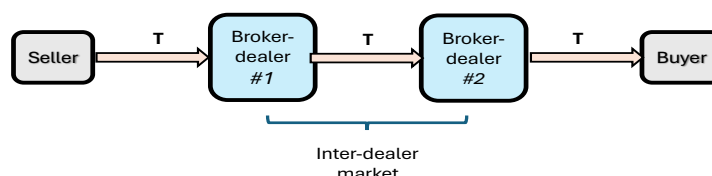


Figure 5: Treasury market transaction chain

We estimate the volume of liquidated Treasuries in the March 2020 event by subtracting the volume that was absorbed by broker-dealers. This amount was \$70-\$75 billion (Fleming et al., 2022).²⁸ Filling in with median reported numbers²⁹ yields:

$$\text{Liquidation volume} = \$500bn/3 - \$72.5bn = \$94bn$$

This indicates that the Treasury market meltdown of March 2020, which was the most severe disruption in decades, involved a selloff of less than \$100 billion. This represents less than 1/2 of one percent of Treasuries held by the public. It underscores the extreme fragility of the Treasury market and explains the subsequent focus by academics, industry participants and regulators to develop proposals to improve Treasury market resiliency. It is approximately 1/3 of the current market value of stablecoins.³⁰

the week of the event. Source: TRACE data (Committee on Capital Markets Regulation, 2021) and (Inter-Agency Working Group on Treasury Market Surveillance, 2021)

²⁶“Traditionally, dealers have been the predominant market makers, buying and selling securities from customers to meet customer trading needs” (Fleming et al., 2016).

²⁷A chain with two broker-dealers is the most frequently occurring chain type in the US Treasury repo market (Aronoff et al., 2026).

²⁸Fleming et al. Chart 13 is a visual representation of confidential FR 2004A Weekly Reporting of Dealer Positions. The value range is based on visual inspection.

²⁹We checked the accuracy of our estimates as follows. The TRACE data show an approximate aggregate daily increase in Treasuries transactions of \$500bn during the week of the “dash for cash”, March 16-20, 2020, relative the average volume during the preceding four weeks. The TRACE data counts every transaction. We divide by 3 to obtain an estimate of net Seller sales. The resulting amount is consistent with the TRACE volume for customer (i.e., non broker-dealer) sales reported in Chart 11 of (Fleming et al., 2022). This coincidence shows that the chain length in Figure 5 is consistent with the data.

³⁰A redemption run will cause an increase in notional sales for Treasuries across the maturity spectrum. This results from a liquidation of a repo position where the stablecoin issuer elects not to “roll over” into a new repo after selling the Treasury at the second-leg. When that occurs the counterparty must find another way to fund its Treasuries—either a repo with a new counterparty (if one can be found) or a sale. The sale will involve Treasuries across the maturity spectrum, which is the composition of repo collateral.

The projected rapid growth in stablecoins, if it materializes, will generate heightened risk of Treasury market disruption in the future. Optimistic forecasts of stablecoin adoption predict a market value of \$2-\$4 trillion by 2030 (Citi Institute, Global Perspectives & Solutions, 2025), which is a nontrivial portion of the \$26-\$27 trillion of the publicly held US government debt currently forecasted for 2030 (Office, 2025). On the evidence of recent disruptions, even a modest uptick in net redemption in the future could dislocate the Treasury market and compromise the ability of stablecoin issuers to maintain par-value.³¹

5.3 Bottlenecks in the Treasury markets

Bottlenecks arise from the intermediated structure of the two Treasury markets. The source of bottleneck in each market is caused by a balance-sheet constraint and a limitation on the volume of central bank reserves available to broker-dealer affiliates of banks.

Secondary Treasury market: limitations on central bank reserves. There are two ways a bank affiliate of a broker-dealer can facilitate the purchase of a Treasury. If the payment is made to a seller account at the subject bank, it increases the seller's deposit account and increases its assets by the value of the acquired Treasury. This pushes its leverage ratio closer to the regulatory limit (see below). If the seller holds a deposit account at another bank, the subject bank is required to send central bank reserves of equal value to the seller's bank. This requires the bank affiliate of the broker-dealer to have adequate reserves on hand. If it runs short of reserves it cannot acquire the Treasury.

Treasuries repo market: limitations on balance-sheet capacity. A broker-dealer acting as repo lender must transfer a bank deposit at the first-leg. This can be accomplished in either of the two ways discussed above, with the same consequences. An additional limitation on intermediation capacity in the repo market arises from the interaction of accounting rules and bank capital requirements. Accounting rules require a broker-dealer to increase recorded assets by approximately the value of the intermediated repo trade, while bank capital regulations limit the permissible increase in assets. An increase in the volume of repo intermediation will move broker-dealer assets closer to the regulatory limit (see below).³²

5.3.1 The supplementary leverage ratio constrains repo intermediation

The supplementary leverage ratio ("SLR") is the bank capital regulation that has imposed the tightest constraint on the ability of banks to allow their broker-dealer affiliates to increase repo intermediation volume during stress events. The SLR places a lower bound, denoted by \underline{L} , on the ratio of bank capital to unweighted

³¹A recent study estimates a 2.5-5 basis point decline in T-bill yields following a \$3.5 billion inflow into stablecoins, which suggests that Treasuries are highly sensitive to stablecoin redemptions (Ahmed and Aldasoro, 2025).

³²Repo trades are treated as secured financing under GAAP rules (See FASB ASC 860-30-25-2 and ASC 860-10-40-5). The first-leg sale of Treasuries causes recorded assets to increase by the sale price. Intermediation involves the first-leg purchase and sale of a Treasury. Therefore, intermediation causes recorded assets to increase. For an example application of the repo accounting rule see (Salerno et al., 2016). For a detailed explanation of repo accounting rules see (Aronoff et al., 2025).

assets plus off balance-sheet exposures, of 3% with an additional 2% for large globally systemically important banks (GSIBs) (Bank for International Settlements, 2010).³³

$$\text{SLR: capital}/(\text{assets} + \text{exposures}) \geq 3\% + 2\% \text{ for GSIBs} = \underline{L}$$

In recent years the largest dealer banks have been operating near their SLR lower bound, which limits their capacity to absorb an increase in repo volume (Table 4).

Bank	SLR, Q3 2025
JPMorgan Chase	5.8%
Bank of America	5.8%
Citigroup	5.5%
Goldman Sachs	5.2%
Morgan Stanley	5.5%

Table 4: Supplementary Leverage Ratio (SLR) for Major U.S. GSIB Dealer Banks, Q3 2025
Source: Corporate 10-Q filings.

The combination of the extremely large volume of recorded assets required to intermediate the \$12 trillion repo market, the low profit margin earned from repo intermediation and the proximity to the SLR lower bound of the major repo intermediaries has prompted concern that the SLR regulation has placed a binding constraint which is limiting the capacity of their broker-dealer affiliates to intermediate the US Treasuries cash and repo markets. In his 2017 Baffi Lecture economist Darrell Duffie expressed concern over the restrictive impact of the SLR on intermediation:

The concern is instead that the amount of intermediation provided by banks to low-risk asset markets has become inefficiently low... the largest U.S. dealer banks must carefully consider the impact of the leverage ratio rule (SLR) on their minimum capital levels when deciding how much of their balance-sheet to allocate to safe asset intermediation (Duffie, 2017), Chapter 2).

5.3.2 The standing repo facility does not relieve balance-sheet constraints to Treasuries intermediation

A feature of the September 2019 repo disruption and the March 2020 secondary market disruptions was the inability of the bank affiliates of broker-dealers to acquire central bank reserves to meet demand. This is superficially striking because of the abundant central bank reserves in the banking system at the time. The problem has been identified as a mal-distribution of reserves, whereby banks with excess reserves could not send those reserves to broker-dealers because there was no active inter-bank lending market and the banks holding excess reserves did not intermediate in the Treasury markets (Copeland et al., 2021; Afonso et al.,

³³The exposures are mostly related to derivatives positions.

2021). The SRF is intended to remedy this by enabling broker-dealers to access reserves directly from the Fed. The SRF enables a bank to sell Treasuries to the Fed at the first-leg in exchange for the reserves it requires to fund the purchase of Treasuries from – in this example – the stablecoin issuer. The bank can thereafter roll over the repo at the second-leg until it finds a buyer for the Treasuries it purchased from the stablecoin issuer. The objective of the SRF, as stated by the Fed, is to avert a meltdown by providing liquidity to broker-dealers to enable them to absorb a surge in selling by market participants (Powell, 2025; Board of Governors of the Federal Reserve System, 2021).

Figure 6 modifies the redemption process depicted in Figure 2 by adding a Step 5 where the Treasury buyer – shown as a broker-dealer – obtains reserves from the SRF, which it uses to complete its purchase of the security from the stablecoin issuer.

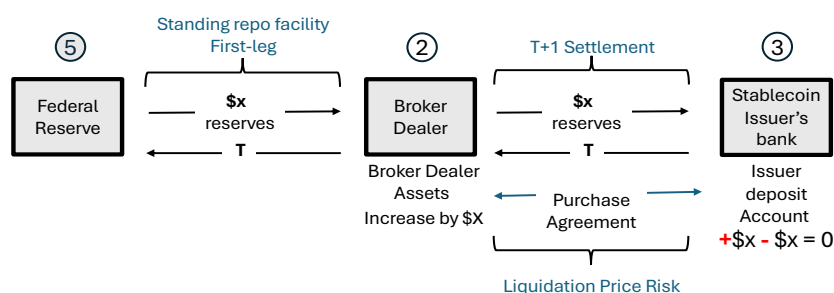


Figure 6: Stablecoin redemption process

When the stablecoin issuer employs a redemption intermediary, such as Circle uses Coinbase and several other firms, these market-makers add another layer to the redemption process. For example Circle would need to liquidate securities – which may not be Treasuries – to acquire the stablecoin from the redeemer. After that, the process is repeated when Coinbase redeems with Circle. It is unclear how the redemption intermediary may affect the demand for central bank reserves. It has a neutral effect when it uses bank deposits to acquire stablecoins and then retains the stablecoin during the stress period. It magnifies demand when it liquidates securities and then immediately redeems with the stablecoin issuer.

Contrary to the stated intent of the SRF, we believe its significance in alleviating market stress is limited. The key thing to note is that in Step 2 the broker-dealer enters into a reverse-repo, which requires it to increase its assets by the amount of reserves it borrows from the Fed. A prohibition on centrally clearing repo trades with the Fed prevents the broker-dealer from netting the reverse-repo with an un-netted repo, to the extent it has un-netted repo volume.³⁴ An analysis by Bowman et al. (2024) concludes that the central clearing mandate, which requires broker-dealers to centrally clear all Treasuries repo and secondary trades (excluding trades

³⁴The Fed is excluded from the central clearing mandate (Securities and Commission, 2023). Central clearing novates initial trades contracts and replaces them with a central clearing counterparty (“CCP”) as the counterparty for each trade. This ensures that trades are multilaterally netted.

with the Fed), will not significantly reduce broker-dealer recorded assets and therefore will not significantly affect their SLR.³⁵ This limits the volume of reserves that broker-dealers can obtain from the SRF, even after the central clearing mandate is implemented.³⁶ Our main conclusion is that the interaction between accounting rules and bank capital regulations, at a time when broker-dealer affiliate banks are operating near their SLR lower bounds, limits the volume of reserves that broker-dealers can obtain from the SRF during a period of market stress, such as when stablecoin issuers are required to liquidate a large volume of Treasuries to maintain par-value. This presents a tangible risk that stablecoin issuers will be unable to meet the par-value requirement at all times.

5.4 Informationally insensitive securities and the risk of stablecoin runs

Here we discuss the other channel of causation; where a modest disruption in the Treasury markets can induce a run to redeem. Holmström (2015) and Dang et al. (2017) posit two interdependent conditions that a security must fulfill to be accepted as a safe asset: (1) that it credibly maintains par-value with central bank money or some other reference asset and (2) that agents do not—and cannot without incurring cost—verify the underlying condition of the assets backing the security. (1) is self-evident. (2) is subtle. Bank deposits satisfy (2) because depositors do not observe the granular composition of loans that comprise the majority of bank assets, or its off balance-sheet derivatives and interest rate exposures. It means that depositors do not know the underlying condition of each loan and exposure. When confidence in the bank’s solvency is high, no depositor has an incentive to try to gain an advantage by spending to become better informed about the bank’s asset portfolio. But when solvency is questioned, confidence quickly evaporates, as occurred in 2023 when SVB’s losses on its Treasuries portfolio was revealed and rendered it insolvent.

Panics happen when information-insensitive debt turns into information-sensitive debt... A regime shift occurs from a state where no one feels the need to ask detailed questions ... to a state where there is enough uncertainty that some investors begin to ask questions about the underlying collateral ... This can lead to reduced liquidity and rapid drops in prices. (Holmström, 2015)

Another example of this phenomenon occurred in 2008 when the Reserve Primary Fund, at the time the largest MMF, “broke the buck” by deviating from par by a mere 3%, which led to mass redemptions and a collapse of the fund. Anadu et al. (2024) documented that both MMFS and stablecoins have experienced runs in response to small deviations from par. This historical causal pattern can be understood by considering the role of broker-dealers in intermediating the Treasury markets (as discussed above). We have seen that a redemption involves a sale of Treasuries to a broker-dealer (to the extent the stablecoin issuer does not have bank deposits on-hand to cover the redemption), and that broker-dealer capacity to purchase Treasuries is constrained by the limitation on the ability of bank affiliates of broker-dealers to obtain additional reserves

³⁵“Combining a detailed analysis of the rules involved in calculating the SLR with a unique set of regulatory data, we conclude that expanding central clearing would have relatively limited effects on the level of SLRs.”

³⁶Recall that repo intermediation increases recorded assets, which pushes the SLR closer to its lower bound.

from other banks or from the SRF. An additional factor is that the remaining capacity of a broker-dealer to purchase Treasuries involves elements that are not visible to outsiders, such as the ability of the affiliate bank to re-allocate reserves to the broker-dealer by making adjustments in other parts of its balance-sheet (“Banks are opaque by design” (Dang et al. 2017)). This opaqueness makes the capacity of broker-dealer intermediaries in the Treasury markets to process transactions informationally insensitive. At most times, stablecoin holders reasonably assume that redemptions can be processed. However, a small disruption in par-value of the stablecoin can signal that broker-dealers have reached the limit of their capacity to facilitate Treasuries purchases, and cause a regime shift where parties lose confidence in the ongoing ability of the stablecoin issuer to effectuate redemptions at par. This, in turn, could possibly trigger a redemption run.

5.5 Stablecoin issuer access to Fed reserves: a solution with complications

A solution: Granting stablecoin issuers access to the Fed discount window or the SRF would improve the ability of a stablecoin issuer to meet redemption requests during a run.³⁷ It would do so by enabling the stablecoin issuer to borrow against Treasuries directly, thereby avoiding a market bottleneck. Direct access is required because, as we explained in Section 5.3, the liquidity provided by the standing repo facility to Treasury market intermediaries does not reliably flow through to provide liquidity to stablecoin issuers.³⁸

Complications: There are two cases to consider.

- (Discount window/ SRF access.) There is no doubt that every firm and household would individually benefit from access to central bank liquidity. However, universal access would create soft budget constraints throughout the economy, which would undermine efficiency (Kornai et al., 2003). The question is whether the Fed should view stablecoins as a form of money for which it has responsibility to provide support. Notably, a condition for direct access would require that stablecoin issuers become subject to bank-type regulations. This could substantively increase operating cost and place into question the viability of stablecoin issuers in a low interest rate environment.
- (No direct access.) An alternative is to allow stablecoin issuers to have “Fed skinny accounts”, as recently described by Fed Governor Waller (Federal Reserve, 2025). While the concept is still speculative, the essential idea is to allow stablecoin issuers to hold non-interest paying central bank reserves without directly transacting with the Fed. On one hand, this would reduce cost and complications involved in redemption and minting transactions. The stablecoin issuer would not be reliant on a third-party bank to intermediate, replacing the stablecoin issuer’s bank with the stablecoin issuer in Figures 2 and 3. On the other hand, this would not solve the bottleneck discussed in Section 5.3, except to the

³⁷Moreover, the existence of such access will reduce the incentive of agents to participate in a run by making them less fearful that a run will threaten the stability of par-value.

³⁸A recently proposed additional source of liquidity that could serve as a backing asset, called PORTS, involves issuance of overnight Treasuries that settle on-chain (Duffie and Wilson, 2025). PORTS would reduce the interest rate risk of holding Treasuries. However, the required daily auction of Treasuries would be subject to the bottlenecks discussed above. Another implication is that PORTS may reduce demand for stablecoins, since it would be an alternative on-chain safe asset.

extent that the stablecoin issuer could hold reserves as a backing asset. It would still have to liquidate Treasuries through market intermediaries.

The diversion of reserves into stablecoin issuer portfolios could have a first-order contractionary effect on the banking system.³⁹

(i) The movement of reserves out of the banking system could reduce lending, which has traditionally been bounded by a minimum reserve ratio.⁴⁰

(ii) The movement of reserves out of the banking system will cause deposits to contract. The reason is that when a stablecoin issuer receives a central bank reserve from a bank as payment for a minted stablecoin or the sale of a Treasury security, the buyer's bank deposit is extinguished, which contracts the volume of deposits in the banking system.

5.6 Summary

Stablecoin issuers are minimizing risk of capital loss and maximizing flexibility to meet redemptions by investing their backing assets in short duration securities (Section 3). Their asset portfolios are more conservative than commercial banks by a long-shot. And yet, they are at much greater risk of defaulting on their monetary liabilities compared to banks. The difference is that banks are integrated into the Fed's monetary system and have direct access to the Fed's balance-sheet in a stress scenario. Stablecoin issuers, by contrast, are exposed to the risk of market bottlenecks which are likely to arise in stressed situations. One solution to the liquidity risk faced by stablecoin issuers is to enable them to borrow reserves from the Fed. However, allowing stablecoin issuers to hold central bank reserves could, depending on the rules, increase costs due to regulatory oversight, disintermediate banks, and reduce lending in the economy.

6 Technical and operational risks

In this section, we explore risks associated with the operation of a stablecoin payment system. The use of a blockchain platform introduces risks that are not present in the incumbent financial system, which is operated on platforms controlled by (central and commercial) banks. We first compare features of a decentralized blockchain with a centralized network of intra and inter-bank payments. We then enumerate technical and operational risks associated with the blockchain itself and its interaction with the smart-contract that holds the stablecoin accounts and executes transfers. After that, we discuss measures that can be taken to mitigate these risks.

³⁹We do not here address second-order effects, which could include Fed open market operations to offset impacts from stablecoin issuer acquisition of reserves. For example, the Fed may increase reserves to maintain a target level of reserves in the banking system when reserves are transferred from banks to stablecoin issuers, or it may reduce reserves to counter the expansionary impact of Fed transfers of reserves to stablecoin issuers via the SRF or discount window.

⁴⁰This is not an issue in the current "ample reserve" regime, but it would re-assert in the future if the Fed shrinks its balance-sheet in line with historical levels.

6.1 Centralized versus decentralized payment platforms

Consensus on transaction finality. A core difference between decentralized blockchains used for stablecoin payments and incumbent bank-operated payment rails lies in the type of “consensus” required to finalize transactions. On a public blockchain, transaction finality is an outcome of a protocol-level consensus mechanism (e.g., proof-of-stake or proof-of-work), in which a distributed set of validators orders transactions into blocks and the network converges on a canonical ledger. Finality may be probabilistic (strengthening with additional confirmations) or economically deterministic once a finality rule is met, but it is ultimately anchored in software rules and incentive compatibility among independent participants. By contrast, bank payment systems rely on institutional trust and governance rather than computational consensus: transactions are finalized when they are accepted under the operating rules of the relevant payment system and settled across bank accounts, often in central bank money. In this setting, settlement finality is primarily a legal and operational concept—backed by supervisory oversight, access controls, and well-defined procedures for exception handling—rather than an emergent property of open-network coordination.

Recourse. These different finality models map directly into differences in responsibility for system operation and the availability of legal recourse when payments are mishandled. In centralized bank platforms, responsibility is clearly allocated: regulated banks, payment system operators, and (for settlement in reserves) the central bank each have defined operational obligations, supervisory expectations, and liability regimes. Errors can often be investigated, reversed, or compensated through established dispute-resolution channels, and regulators can demand remediation through examinations and enforcement actions. In decentralized stablecoin payments, operational responsibility is more diffuse. Validators provide the ordering service but typically do not have a customer relationship with end users; smart contracts may execute transfers automatically with limited scope for ex-post intervention; and failures can arise from software vulnerabilities, governance attacks, key compromises, or outages at intermediaries such as wallets and exchanges.

Record-keeping. These differ in ways that matter for transparency, auditability, privacy, and supervisory access. In a stablecoin system implemented on a public blockchain, the ledger of token ownership and transfers is typically maintained as a shared, append-only record, and the issuer’s liability to token holders is represented by balances in a smart contract. This can make transactional histories widely observable, machine-verifiable, and reconciled by design. In incumbent bank payments, by contrast, customer deposits and intrabank transfers are recorded on bespoke internal ledgers maintained by each institution, while interbank payments are reconciled through centralized messaging and settlement arrangements; the central bank and payment system operator maintain authoritative records of reserve balances and the settlement positions of participating banks. The result is a layered accounting architecture that is less publicly transparent than a blockchain ledger and requires costly reconciliation, but embeds clear permissioning, confidentiality, and supervisory controls.

6.2 Stablecoin infrastructure risks

Incentive risks. Many stablecoins rely on public proof-of-stake (PoS) blockchains where validators are rewarded (fees and token issuance) for producing blocks and can be penalized (“slashed”) for violating protocol rules. For regulators, the key point is that transaction finality and throughput are delivered by an incentive system rather than by a supervised operator with an explicit contractual responsibility to provide neutral, continuous service. Validators typically have discretion over transaction ordering and can prioritize transactions that maximize revenue, including through maximal extractable value (MEV). In normal conditions, this can affect fairness and predictability for payment users; in stress, coordinated delay or censorship can occur and produce “liveness” failures in which the network remains online but does not reliably process transactions. These dynamics can impair payments without a clear liability framework or guaranteed remediation pathway comparable to those in regulated payment systems.

Transaction processing risks. A stablecoin might not be able to maintain par-value if users cannot reliably transfer tokens or if the stablecoin issuer cannot reliably mint and redeem. On-chain, these functions are simply transactions; if the underlying network is congested, attacked, or otherwise unable to process transactions, transfers and issuer operations may be delayed or fail. Operational impairment can quickly translate into financial impairment: reduced transferability undermines the stablecoin’s usefulness as a medium of exchange, and impaired redemption can widen secondary-market discounts and amplify run dynamics. In addition, issuer-controlled smart contracts introduce issuer-side operational risk, including software defects and weak administrative controls over minting and burning. For example, in October 2025, Paxos mistakenly minted \$300 trillion of PYUSD and corrected the error with an offsetting burn within minutes; Aave paused PYUSD activity and PYUSD briefly traded about 0.5% below par before stabilizing.⁴¹ The regulatory relevance is that some drivers of impaired transferability and supply control are within the stablecoin issuer’s governance (contract design, key management, multi-party approvals, caps and rate limits, incident response), while others arise externally at the blockchain’s consensus and network layers.

Quantum threats. Most major blockchains rely on signature schemes such as ECDSA or EdDSA that are not considered quantum-resistant. A sufficiently capable, error-corrected quantum computer running Shor’s algorithm could in principle derive private keys from public keys and authorize fraudulent transfers, enabling theft at scale and undermining confidence in the ledger. Although a cryptographically relevant quantum computer (CRQC) is not known to exist and timelines are uncertain, the issue is preparedness for a low-probability, high-impact transition that could disrupt payment continuity if not executed in an orderly fashion. Post-quantum standards are emerging (including NIST post-quantum cryptography standards), but public blockchains would still require coordinated protocol upgrades, wallet support, and migration of assets to new cryptographic primitives (NIST, 2025; Parida et al., 2023). Note that should a CRQC become

⁴¹The erroneous mint of 300 trillion PYUSD happened on the Ethereum blockchain on October 5th, 2025 at 7:12:23 PM UTC and the related burn of 300 trillion PYUSD happened at 7:34:35 PM UTC, a span of just under 23 minutes. Mint transaction hash: 0xc45dd1a77c05d9ae5b2284eea5393ecce2ac8a7e88e973c6ba3fe7a18bf45634 Burn transaction hash: 0xaa532ae7f06ccdbdc226f59b68733ae8594464a98e128365f8170e305c34f4b

practical, it would have a broad impact beyond the public blockchain ecosystem. Impacted areas would also include the traditional financial system as well as communications, government, military, healthcare, and other critical infrastructure. For policymakers, the relevant question is whether stablecoin arrangements have credible governance and operational plans to execute such a migration without jeopardizing users' ability to transact and redeem at par, especially given that stablecoin issuers and operators do not control the underlying blockchains.

Technical risk framework. There are several categories of stablecoin risk that can impact par-value. A stablecoin can suffer from an unrestricted change in token supply. This can render the stablecoin issuer insolvent if liabilities are increased without a corresponding increase in assets. A stablecoin can suffer network liveness faults where it lacks the ability to process transactions. This undermines the usefulness of the stablecoin as a medium of exchange. A stablecoin can also suffer from logic bugs, administrative key compromise and other operational issues. Some effects can be limited to a small number of transactions while others can have universal impact. Some of these risks are controllable by the stablecoin issuer while others are imposed externally.

The following table presents a matrix that covers the probability and potential impact of various technical stablecoin risks. We classify risks by probability and potential impact in order to clarify the types of technical failures that could cascade into broader financial impact. We also indicate which risk is controllable by the stablecoin issuer (I), which are externally imposed (E) and which are shared between the two (I/E). MITRE's AADAPT knowledge base IDs, which categorize adversary techniques for digital asset management systems, are included if available.⁴²

High systemic risk relates to issues which impact both the control of the supply and the liveness of the entire system. Faults in this class can impact all users and result in the most financial loss. Low systemic risk only impacts liveness and does not pose uncontrolled supply issues.

⁴²MITRE AADAPT™ (Adversarial Actions in Digital Asset Payment Technologies) Framework: <https://aadapt.mitre.org>

	Most Likely	Moderately Likely	Least Likely
High Systemic Risk	<ul style="list-style-type: none"> Smart Contract Logic Flaws (I) AADAPT: ADT3012 Bridge Failure (I/E) AADAPT: ADT3029 	<ul style="list-style-type: none"> Flash loan pricing attacks (E) AADAPT: ADT3015 Administrative key custody failures (I) AADAPT: ADT1552 Contract Upgrade Failures (I) 	<ul style="list-style-type: none"> Consensus Attacks (E) AADAPT: ADT3013 Cryptographic Exploits (E) Compiler bugs (I/E) Integration bugs (I) Validator coercion (E)
Medium Systemic Risk	<ul style="list-style-type: none"> Centralized Infrastructure Failure (I/E) AADAPT: ADT3008 DDoS Attacks (E) 	<ul style="list-style-type: none"> Governance Attacks (E) MEV Exploitation (E) 	<ul style="list-style-type: none"> Replay attacks (I/E)
Low Systemic Risk	<ul style="list-style-type: none"> Liquidity Pool Imbalances (E) Front-Running (E) Slippage beyond tolerance windows (E) 	<ul style="list-style-type: none"> L2 Specific Vulnerabilities (I/E) Gas Price Manipulation (E) Block stuffing to force higher fees and/or censorship (E) 	<ul style="list-style-type: none"> Block Reorg Attacks Time-based Vulnerabilities (E) AADAPT: ADT3003 Function signature mismatches (I/E)

Figure 7: Technical Risk Matrix

Smart contract logic flaws can result in uncontrolled supply and transactional liveness issues. Upgradable stablecoin smart contracts are also vulnerable to logic issues introduced via the upgrade process. They are vulnerable to upgrade credentials becoming known externally, resulting in a catastrophic loss of issuer supply control and network liveness. Both of these risks are within the control of the stablecoin issuer but must be mitigated before contract deployment.

Bridges operate across stablecoin networks and include the ability to alter the supply on these networks. Loss of a bridge can cause deposit and redemption liveness issues while bridge takeover or key exposure can result in uncontrolled supply. Control over this risk exists when the bridge is operated by the stablecoin issuer, but some bridges are operated externally.

A flash loan is a form of riskless lending that is taken out and repaid in the same moment which can be used to amplify an economic attack. They can be leveraged to increase the magnitude of price dislocations in decentralized markets. This could be used in extreme cases to alter the value of base layer tokens impacting consensus incentives, or alter the value of reference prices in algorithmic stablecoins. Flash loans are unique to blockchains and not within the control of the stablecoin issuer.

Consensus and validator attacks primarily result in censorship and transactional liveness faults and are outside the control of the issuer. However, in the extremely rare case of a $> 2/3$ consensus takeover of a PoS chain by an attacker with large compute resources, uncontrolled supply is also possible. In this case, an attacker obtaining keys from exited validators can create an alternative history including altered mint transactions. However, this would trigger a detectable chain split which should be rejected by the community.

Smart contract compiler and integration bugs are not very likely but pose both transactional liveness and uncontrolled supply issues, making them highly systemically risky. However, like smart contract bugs, mitigation of this risk exists with the stablecoin issuer.

Cryptographic exploits and network layer compiler bugs impact both blockchain and traditional systems. The recourse in a permissionless blockchain based system involves human governance actions which are not clearly defined. These issues impact both transactional liveness and the control of supply.

Validator coercion impacts transactional liveness and in extreme cases, control over the supply. Both blockchain based and traditional systems suffer from centralized infrastructure failure and distributed denial of service (DDoS) attacks. Governance attacks primarily impact supply control and this risk is outside the control of the stablecoin issuer. MEV exploits are a type of deliberate front-running which also primarily impacts transactional liveness. Replay attacks where a single transaction is valid on more than one blockchain are not very likely but possible if a contentious hard fork of the network is made without adequate countermeasures.

All of the other low systemic risks are outside the control of the issuer.

6.3 Technical risk mitigation

A stablecoin issuer can reduce its controllable risks on public permissionless blockchains through practices including testing, auditing, monitoring, and implementation of operational best practices. These measures lower the likelihood of failure, but they cannot completely eliminate technical risk. We now turn to measures that reflect industry best practices for the development, testing, deployment, and monitoring of a stablecoin issuer's smart contracts.

6.3.1 Smart contract layer and administration

Stablecoins are implemented using smart contracts, which are software programs executed by the blockchain's nodes. As stablecoin issuers develop the underlying smart contracts, they must properly architect these programs and mitigate the risk of introducing bugs that could impair the stablecoin's functioning. Software bugs are among the most fundamental and significant potential vulnerabilities in a stablecoin's deployment and use. Typically, stablecoin issuers must first conduct internal testing of the source code, followed by external assessments by independent smart contract auditing firms, before the code can be deployed live to support transactions.

The stablecoin issuer should also maintain distinct environments for development, staging, and production, and consider how they administrate the smart contracts, including key management and access controls.

Development and testing. As developers contribute to the smart contract code base, comprehensive testing should be employed. This testing of the underlying code must be thorough and evaluate each unit (a single component of the smart contract), its integration into the stablecoin issuer's broader platform (testing of the interaction between units), and fuzz testing (probing how the system behaves when it receives unpredictable inputs). Formal verification for critical contract components is encouraged where practical.

After internal testing is complete and before deployment or upgrade, stablecoin smart contracts should be audited by multiple independent smart contract auditing firms to identify any remaining software bugs. Using common, well-understood libraries reduces auditing demands by shrinking the attack surface, since those libraries have already been extensively audited.

Deployment. It is an industry best practice for the stablecoin issuer to deploy an upgradable smart contract so it may be revised later to address potential bugs or support future expansion.

To avoid the introduction of erroneous or malicious code, upgradable contracts may be deployed with appropriate time locks and multi-signature requirements. Time locks delay the smart contract's actual deployment, creating a window for additional review, allowing identification of irregularities and for response systems to mitigate them. Multi-signature arrangements require approval from multiple internal parties to activate the new contract. By bringing in multiple reviewers from different parts of its operations, the stablecoin issuer can reduce the risk of inadvertently deploying bugs to the blockchain.

Circuit breakers. Stablecoin issuers need administrative functions such as the ability to halt live operations in the event of significant anomalies. While issuers build manual kill switches into the smart contract code, they should also develop circuit breakers that automatically stop transactions that are clearly out of bounds, such as minting an exceptionally large number of tokens. These stopgap functions constrain the magnitude of damages once a process runs awry. The stablecoin issuer may gradually increase caps and limits as the system proves its stability.

Administrative and compliance operations. Once a smart contract is deployed, the stablecoin issuer must be able to perform administrative tasks, such as minting, burning, or pausing transactions. They also must be able to manage the blocklist of addresses that are not permitted to be involved in transfers of the stablecoin, and to upgrade the contract when needed. There is a misunderstanding about what it means when it is said that blockchain-based stablecoin transactions are "peer-to-peer." Note that the stablecoin issuer's smart contracts must process any on-chain stablecoin transaction. Currently, stablecoin issuers are not required to intermediate stablecoin blockchain transactions. This is a point where a stablecoin issuer could intermediate in transactions, if compelled to do so.

Administrative access controls. To carry out the above operations safely, issuers should use robust access controls, such as multi-signature approval schemes with appropriate thresholds and a diverse set of signers

who approve changes to those operations. Time-locks can provide an additional safeguard for sensitive actions, and clear key-management procedures, including the use of hardware security modules (HSMs), help prevent operational errors. Separating routine operational keys from emergency-only keys further limits the impact of any compromise of internal controls. Defense-in-depth security practices, regular assessments of administrative infrastructure, and careful documentation of all administrative actions contribute to a more resilient stablecoin system.

Bug bounties. Even after developing, testing, and auditing new code, some problems may remain undetected until the code is deployed on a blockchain. Any external party can audit smart contracts because they are publicly visible, which increases trust in the system and encourages more reviews of the underlying code. Nonetheless, any issues public stakeholders identify can be rapidly exploited if the external party that spots a problem does not share this information with the stablecoin issuer first. Incentives for the responsible disclosure of any problems external parties may discover increases the speed at which the stablecoin issuer can address vulnerabilities in the code. This can be partially mitigated by maintaining bug bounty programs with meaningful rewards.

All of these strategies reduce the incidence of software bugs, whether introduced erroneously or maliciously.

Bridges. A bridge smart contract enables transfers of a stablecoin between supported blockchains. The ability to move stablecoins from one blockchain to another expands the range of counter-parties with whom a stablecoin holder can transact. Some stablecoin issuers run their own cross-chain services to move stablecoins, but there are many third-party bridges which do not appear to have contractual relationships with stablecoin issuers, and to-date, stablecoin issuers do not necessarily license or permission bridges and thus do not have influence into how they operate.

Bridges function by synchronously swapping the ownership of funds on one chain with an equal amount on another. They may do this by accepting assets into the control of the bridge operator on one chain and pay that same amount of assets out of their inventory to the same customer on another blockchain. Alternatively, if operated by the stablecoin issuer they may burn value on one blockchain and recreate that same value on another blockchain. In these cases where bridges automatically mint and redeem assets on multiple blockchains, they represent a high systemic risk to the stablecoin issuer.

As with smart contract upgrade concerns, a large degree of this bridging risk can be mitigated in the same ways: bridge builders must conduct thorough testing, use third-party auditing, and may employ time locks, but solutions must be automated and avoid routine manual interventions. For example, if a transaction exceeds a certain threshold, the stablecoin issuer could time-lock the transfer so that it is unusable for a period, allowing for mitigation of a mistaken or malicious attempt to initiate a large transfer of stablecoins. Additionally, a stablecoin issuer may implement an upper-bound limit on the amount any particular stablecoin can be bridged over some limited time frame.

6.3.2 Blockchain layer

Stablecoins run on public, permissionless blockchains, whose primary feature is that they are not governed by a single or small set of actors.⁴³ This is quite different than how the traditional financial system operates, and means that there are many technical risks that are not under a stablecoin issuer's control.

Consensus. A blockchain's consensus process determines which transactions become part of the authoritative ledger and when they can be treated as final. In proof-of-stake⁴⁴ systems, validators (independent operators running specialized software) check transactions against protocol rules, assemble them into proposed blocks, and then attest to whether those blocks should be accepted by the network. For stablecoin payments, this layer is not a technical detail: it directly governs settlement finality, throughput, and the conditions under which transfers can be delayed or excluded.

Consensus security depends on the validator set being meaningfully decentralized. Because voting power can be concentrated through stake, a single entity can effectively "collude" by controlling many validators, even without coordination among separate firms. If a dominant validator or cartel gains sufficient influence, it can censor otherwise valid transfers, reorder transactions for profit, or weaken reliability during stress—all of which can impair payment continuity and undermine confidence in stablecoin par-value exchange. We explain this dynamic in more detail in Section 7.1.

Risk mitigation starts with chain selection and operational discipline. Stablecoin issuers should monitor stake and voting concentration, governance changes, and validator behavior that could indicate censorship or instability. They should apply conservative finality requirements (and, where appropriate, longer confirmation thresholds) before crediting high-value redemption transfers. While proof-of-stake protocols can penalize misbehavior through slashing, this is not a substitute for prevention. Resilience is strengthened by diverse validator participation, multiple independent client implementations (to reduce correlated software faults), and clear escalation channels with major validators and ecosystem operators when rapid coordination is required.

Monitoring. Stablecoin operations require continuous monitoring and an incident-response capability that is credible under stress. Stablecoin issuers should treat blockchain-facing operations as critical payment infrastructure. They should maintain real-time visibility into network health (finality delays, congestion, reorg risk signals), contract and key activity (mint/burn events, admin calls), and dependencies such as custodians, wallet integrations, and Remote Procedure Call (RPC) providers. Equally important are predefined

⁴³Though this is the stated goal, several so-called permissionless blockchains are in fact controlled by a small set of actors; usually a non-profit foundation partnered with a for-profit company. These actors often hold significant amounts of the blockchain's native token, run or strongly influence most of the validators in the network, and thus can direct or coordinate changes to blockchain-native issuance and protocol upgrades. Interestingly, in these cases some risks are exacerbated (it is easier for validators to collude to censor) while others are less of a concern (in the event of a bug or attack, it is easier for validators to cooperate to roll back errant transactions). It is common for these organizations to compensate the largest stablecoin issuers to get them to issue their stablecoin on their blockchains, implying the potential for other types of contractual relationships, perhaps to manage risk.

⁴⁴Most major stablecoins operate on proof-of-stake blockchains.

response playbooks, secure communications for rapid coordination, and routine security testing (including independent assessments and controlled penetration exercises) to validate that controls work in practice.

Monitoring should also cover consensus-layer attack patterns that may not appear as conventional software failures. For example, “long-range” attacks in proof-of-stake designs can arise if keys from past validators are compromised and used to sign an alternative historical chain in which the attacker has no stake at risk. While modern protocols include defenses, early detection of anomalous reorganizations, inconsistent checkpointing, or unexpected finality behavior is essential to limit user harm, preserve operational continuity, and support timely supervisory reporting.

Infrastructure. To issue and administer an on-chain offering, stablecoin issuers must operate infrastructure that can reliably observe the blockchain and submit transactions (routine and administrative). This infrastructure should be redundant, geographically distributed, and designed to fail over safely such that the issuer does not lose the ability to redeem, manage supply, or respond to incidents during localized outages or provider failures.

Most issuer interactions occur through nodes and RPC endpoints, which can become choke points during market stress. Infura, for example, provides widely-used RPC endpoints. Public-facing endpoints should be protected against denial-of-service attacks, and issuers should maintain multiple, independent RPC and node providers (or self-hosted capacity) with regularly tested failover and disaster-recovery procedures. Routine resilience testing matters as much as architecture: backup systems that are not exercised may fail when needed.

Finally, operational controls around privileged access are central to safety and soundness. Administrative keys and infrastructure accounts should be governed by strong access controls, separation of duties, robust logging, and secure custody arrangements (e.g., multi-party approval and hardened key storage). These measures reduce the likelihood that a single compromise, configuration error, or insider action escalates into a supply-control incident or a prolonged disruption of payments—but they do not eliminate risk, underscoring the importance of layered defenses.

7 Interactions between financial and software risks

In this section we discuss how incentive risks relating to how a blockchain and stablecoins interact could cause additional problems. First, we emphasize that attacks on a blockchain will affect stablecoin management and redemption even if the issuer is not in financial distress; an attacker could censor administrative actions on the stablecoin’s smart contract or user transactions trying to redeem, affecting par-value. Second, we discuss how a stablecoin with large transaction volumes might increase the incentive for an attacker to subvert the underlying blockchain, bringing forth these very attacks. Third, we point out that large stablecoin issuers, like any centralized custodian of tokenized assets, can have influence on blockchain governance, threatening the prospect of credible neutrality. Finally, we point out DeFi’s dependence on stablecoins and

how an attack on a widely used stablecoin might have cascading negative effects on DeFi protocols.

7.1 Stablecoins' vulnerability to underlying blockchain attacks

An inability to complete transactions in a timely fashion compromises the usefulness of stablecoins as a medium of exchange. A loss of liveness, or an increase in the perceived risk of such a loss, can undermine confidence in the stablecoin and trigger a redemption run. This can overwhelm the ability of the stablecoin issuer to maintain par-value, for reasons discussed in Section 5. Moreover, insofar as a loss of liveness affects all transactions on a blockchain, it can trigger a correlated redemption run among all stablecoins. As discussed in Section 6.3.2, the underlying blockchain consensus protocol determines which transactions are processed and in what order. Therefore, stablecoin management and transfers could be impeded by attacks on the underlying blockchain. For the purposes of illustration, we focus on blockchain attacks on Ethereum and its underlying PoS protocol, but it is important to note that these types of attacks are not unique to Ethereum.

There are several classes of attacks on Ethereum's post-Merge PoS protocol which have been studied and identified that would degrade liveness or impede transaction finality. Among them are (i) timing-based and vote-propagation attacks that exploit minor network delays to prevent the formation of a supermajority and a balancing attack and that creates uncertainty about which of two competing chains will ultimately finalize by eclipsing a portion of the network (Neu et al., 2020; Schwarz-Schilling et al., 2021), (ii) secret-chain reorganization attempts, in which an attacker with a supermajority of stake privately constructs an alternative chain and releases it strategically when the financial incentive is greatest (Neuder et al., 2021) and (iii) public competing-chain attacks, in which an attacker broadcasts an alternative chain in real time to generate temporary uncertainty over finality (Schwarz-Schilling et al., 2021).

There is a particularly pernicious attack that is specific to stablecoins and which has not (to our knowledge) been heretofore studied. It involves a combination of a double-spend attack combined with censoring an administrative transaction from a stablecoin issuer to suspend the transfer by blacklisting the attacker's address or pausing the overall contract. If an attacker can censor the stablecoin issuer administrative action, it can act unopposed. The goal of the attacker in each type of attack is to induce the victim to deliver her item of exchange to the attacker and then to nullify the transfer of ETH or the stablecoin. Notably, in some cases the attacker can accumulate transactions before triggering the nullification, with the attacker double-spending several counterparties.

An attacker could censor transactions or halt the chain (affecting liveness) with only slightly more than 1/3 of the underlying stake. An inability to complete transactions in a timely fashion compromises the usefulness of stablecoins as a medium of exchange. A loss of liveness, or an increase in the perceived risk of such a loss, can undermine confidence in the stablecoin and trigger a redemption run. This can overwhelm the ability of the stablecoin issuer to maintain par-value, for reasons discussed in Section 5. Moreover, insofar as a loss of liveness affects all transactions on a blockchain, it can trigger a correlated redemption run among

all stablecoins.

Table 5 in Appendix B compiles a pattern of significant declines in cryptocurrency prices following attacks on the associated blockchain (the examples are not limited to Ethereum). This response reflects a loss of confidence in the integrity of the blockchains. It is plausible that a stablecoin operating on an attacked blockchain would experience a similar loss of confidence from an attack.

A disruption to the functioning of the blockchain will disrupt the execution of stablecoin transactions that are dependent on the functioning of the blockchain. An attack severe enough to cause a loss of confidence in the underlying blockchain token might cause a loss of confidence in the stablecoin by at least some percentage of holders, who would exit by redeeming their stablecoins.

7.2 An increase in stablecoin volume can incentivize attacks on the blockchain

The attacks described above rely on a large amount of stake colluding to conduct the attack. The incentive to collude increases as the potential reward increases. This reward is the amount gained by disrupting the blockchain (a double spend or the profits from a short on ETH) minus the cost to conduct the attack (primarily, the cost of the slashed stake). Note that the latter is denominated in the underlying blockchain token, ETH, while the former could be denominated in the stablecoin. As stablecoin transaction volume rises, the opportunity for double spends in the stablecoin increases, while there is not necessarily a corresponding increase in the punishment for conducting an attack. The cost to mount the attack does not scale with the economic value transacted on Ethereum, but the expected reward does.

The result is a structural vulnerability: as stablecoin activity scales, the prospective gains from manipulating transaction settlement, delaying finality, or creating transient forks grow more rapidly than the honest-validator reward rate. Even if the likelihood of these attacks remains low under normal conditions, the economic incentive gradient steepens with stablecoin adoption. The combination of attack vectors that degrade liveness or obscure finality and the rising value at stake in stablecoin transactions implies that Ethereum's post-Merge PoS chain will become increasingly attractive to adversaries as stablecoins scale.

7.3 Large stablecoin issuers might influence blockchain governance

As others have noted, stablecoin issuers might have unexpected influence on blockchain upgrade and governance decisions because in the event of a blockchain fork due to disagreement, they can choose which side of the fork to honor for stablecoin redemptions (Lee and Qureshi, 2019; Narula, 2021). It is unclear how this might influence governance decisions as stablecoins grow ever larger, and potentially even eclipse the monetary base of the underlying blockchain's native token. If a large stablecoin issuer has this influence, it reduces the credible neutrality of the underlying blockchain as an infrastructure layer. The stablecoin issuer might be required to choose the fork in alignment with the legal jurisdiction in which they operate.

7.4 DeFi’s dependence on stablecoins

Stablecoins are widely used in DeFi smart contracts. For example, there is over \$270 million of USDC in Uniswap pools on Ethereum (Uniswap, 2025). If USDC were to suffer an attack, there might be a run on the stablecoin and many people might rush to withdraw from these pools. Other work has shown that this can serve as a channel for financial contagion in the DeFi sector (Du et al., 2025).

7.5 Summary

Financial and software risks reinforce one another in ways that can undermine the stability of a stablecoin. Disruptions to the blockchain can delay redemptions or transfers, weakening confidence in the stablecoin’s reliability as a medium of exchange and amplifying run risk. Rising stablecoin volume increases incentives to attack the host blockchain by raising the prospective gains from controlling transaction processing. Large stablecoins can influence blockchain governance and cause vulnerabilities for DeFi protocols. Together, these channels illustrate how blockchain-level vulnerabilities can endanger the financial stability of stablecoins, and vice versa. Crucially, many of the vulnerabilities reviewed here are outside the control of the stablecoin issuer and therefore cannot be mitigated by the stablecoin issuer. They arise from the consensus mechanism that underlies a permissionless blockchain.

8 Regulatory safeguards and outstanding policy questions under GENIUS

8.1 Strengths of the GENIUS framework

As addressed earlier in this paper, the GENIUS Act establishes the initial federal architecture for issuing and supervising payment stablecoins. Its strengths lie primarily in its efforts to shape the financial infrastructure underpinning a stablecoin. The Act defines licensing requirements for payment stablecoin issuers, imposes a strict reserve-backing asset requirement, and identifies eligible instruments for reserve backing assets. These constraints sharply limit credit risk and restrict exposure to long-duration securities, which, in turn, may enhance solvency and liquidity, respectively. Monthly public disclosures of reserve backing asset composition and valuations further strengthen transparency and allow market participants to assess issuer risk on an ongoing basis. GENIUS’s prohibition against the rehypothecation of customers’ assets and its requirements for independent audit attestations reduce the risks that opaque leverage or undisclosed exposures build up inside backing asset portfolios.

While the GENIUS Act is now law, regulatory agencies must transpose its principles into tangible regulation, and several provisions in the Act explicitly require further study. Relevant U.S. regulatory agencies must interpret the statute, issue regulations, and build a framework for licensing, supervision, enforcement, and technical standards. Beyond immediate prudential rules, the Act mandates several formal studies, including analyses of potential capital requirements, oversight structures, and the financial stability implications of stablecoin growth. These provisions acknowledge that refinements may be necessary to the regulatory

framework as stablecoin adoption expands and as the interaction between market infrastructure and digital asset regulation becomes clearer.

8.2 Remaining gaps, structural dilemmas, and unresolved questions

While GENIUS addresses reserve backing asset quality and transparency, it leaves several foundational issues unresolved.

First, although the GENIUS Act requires issuers to disclose a redemption policy and to establish procedures for the timely redemption of stablecoins (12 U.S.C. § 5903, 2025), it does not specify how redemptions should work. As discussed in Section 2, this is problematic because most stablecoin holders today cannot redeem their coins directly with issuers. Instead, holders rely on intermediaries such as cryptocurrency exchanges (e.g., Binance or Coinbase), where par value redemption is not assured. At market exchanges, prices for redeeming stablecoins fluctuate with supply and demand.

Some issuers do offer 1:1 redemption to holders who have verified financial accounts with the issuer, but that access is tightly restricted. For example, Circle limits direct redemption to 521 entities and Tether limits redemption to six entities (Ma et al., 2025). These entities act as minting and redemption intermediaries between the stablecoin issuer and other owners of stablecoins.

If regulators permit the current approach to redemptions to continue, the existing two-tiered system will remain. Institutional clients (such as those that have verified accounts with stablecoin issuers) will be able to redeem their coins directly with the issuer, most likely at par. Others, such as most retail customers, will depend on the peg holding in the secondary market. In times of market stress, the value of a stablecoin may fall below par in secondary markets, as it did for USDC during the Silicon Valley Bank crisis (Huang et al., 2023). The only way out for many retail owners of stablecoins in such situations may be to sell their coins at a loss on the open market.

Moreover, frictions arise when issuers must liquidate U.S. Treasury securities through broker-dealer intermediaries that are constrained by balance sheet and leverage ratio requirements. These constraints can impede orderly liquidation precisely when redemptions surge.

In light of recent research documenting systematic and persistent deviations from par in secondary markets (Ma et al., 2025), the GENIUS Act's omission of any reference to maintaining par-value exchange in the secondary market (where most stablecoin users actually transact) raises concerns about whether stablecoins will maintain the public's confidence over the long run.

Second, although the Act requires further study of capital standards, it appears to restrict U.S. regulators from applying directly to stablecoin issuers the minimum leverage and risk-weighted capital requirements that govern commercial banks, as noted in Section 4. Likewise, GENIUS is silent on the dilemma analyzed in Section 5.5: whether stablecoin issuers should have access to Federal Reserve liquidity facilities. Granting

such access could materially reduce redemption-related liquidity bottlenecks. Yet doing so raises complications for monetary policy transmission, the boundary between banks and nonbanks, and the distribution of reserves in the financial system.

Even though stablecoin issuers face run-risk dynamics akin to banks and money-market funds, the GENIUS Act potentially enables a regulatory asymmetry: stablecoin issuers are expected to maintain par-value but are not required to adopt structural protections such as capital buffers or be permitted to access public backstops that support issuers of other forms of demandable liabilities that are expected to honor par-value exchange.

Third, the GENIUS Act authorizes regulators to prescribe interoperability standards for stablecoins, but it does not define what interoperability actually means in practice. As a starting point, interoperability can be broken down into two components, namely network interoperability versus monetary interchangeability.

Network Interoperability asks whether a stablecoin can be used across multiple blockchains, wallets, and platforms without friction. Because the GENIUS Act does not require issuers to support technical standards across chains or wallets, the Act’s silence on the matter creates a risk that stablecoins will operate in isolated silos. For example, a stablecoin on Ethereum might not interoperate with the Solana version of that stablecoin. The BIS has warned that a stablecoin issued on different blockchains may not interoperate cleanly (Committee on Payments and Market Infrastructures, 2023). Without guidance, the U.S. could end up with a digital dollar landscape badly fractured by incompatible technical standards, which could affect liquidity depth and user experience.

Monetary Interchangeability asks whether different USD-based stablecoins are exchangeable with each other at par. Beyond technical standards, however, lies a deeper issue of monetary interchangeability. This is the idea that all stablecoins, like all dollars, should be usable at equal value: ideally a dollar should always be worth a dollar, regardless of its form, whether it is held as a bill, in a bank account, or as a stablecoin. There are many structures in our monetary system to try to ensure this for commercial bank deposits (though it doesn’t always hold all the time). The BIS argues that many stablecoins fail this “singleness of money” test because they are not always redeemable at par or interchangeable across users (Shin, 2025).

The GENIUS Act does not address

- whether stablecoins from different issuers should be fungible, or
- how to ensure par-value exchangeability between similar stablecoins.

This omission opens the door to a potentially fragmented and fragile payment landscape. Some observers compare this potential outcome to the “Wildcat Banking” era in U.S. history, when private banks issued their own banknotes that traded at varying discounts (Gorton and Zhang, 2023). A more nuanced view by Carter (2025) suggests stablecoins could evolve toward a model of competitive digital dollars, where interoperability standards and issuers determine trust. Such an outcome might deviate from the singleness of money in two respects: First, there would be no assurance of acceptance of any given stablecoin as

payment, and second, differences in valuations would imply deviations from par-value.

Finally, the GENIUS Act is silent on the technical infrastructure underpinning stablecoins. To date, stablecoin issuers decide for themselves whether to obtain their own technical audits and may claim to follow best practices, but this approach lacks transparency, accountability, and enforcement. The GENIUS Act advances no requirements for technical audits, open-source transparency, or even secure key management. Furthermore, the stablecoin ecosystem is highly integrated across many infrastructure layers, like wallets and bridges, which have been frequent targets of attacks in crypto markets. Without minimum risk standards for these technical integrations, GENIUS Act-compliant stablecoins may still be vulnerable. It remains to be seen whether regulatory agencies will fill those gaps to strengthen public confidence in stablecoin issuers and the underlying infrastructure they depend upon.

Failing to address these technical concerns risks creating a stablecoin that may be legally compliant, but technically insufficient. Where something does go wrong, there's no clarity about who might be responsible or whether redemptions would still be enforceable.

In summary, GENIUS establishes a strong foundation for backing asset safety and transparency. It leaves open many critical questions about liquidity support, redemption mechanics, capital adequacy, interoperability, technical infrastructure, and the long-run integration of stablecoins into the monetary system. In fairness, regulators have not yet issued proposed rulemakings at the time of this writing, and, consequently, they may mitigate some of the challenges we note here. This discussion above serves as an (incomplete) list of additional areas that need to be addressed.

9 Conclusion

Stablecoins promise to expand the reach of dollar-denominated payments by combining the monetary reliability of traditional assets with the programmability and interoperability of digital networks. The GENIUS Act establishes the first comprehensive federal framework governing these instruments, setting clear conditions for issuance, backing assets, and transparency. Yet the analysis in this paper shows that the stability of GENIUS-compliant stablecoins hinges on how financial risks, technological risks, and regulatory constraints interact—especially under stress.

We first demonstrated that the core financial vulnerability lies in the tension between par-value redemption and market intermediated liquidation of Treasuries. Stablecoin issuers can mitigate the risk of capital loss by investing in reverse-repos. However, to the extent that stablecoin issuers hold Treasury securities, their ability to redeem at par depends on executing timely asset sales through broker-dealers whose balance sheets are themselves constrained by leverage rules and liquidity regulations. Episodes of fragility in the Treasury and repo markets show that even modest surges in selling pressure can overwhelm intermediation capacity due to the fact that the bank affiliates of the largest broker-dealers operate near the regulatory lower bound of their supplementary leverage ratio. This limits their ability to increase balance-sheet assets to accommodate

purchases of Treasuries, either by creating a bank deposit for the stablecoin issuer, or by obtaining central bank reserves, from the Fed’s standing repo facility, to transmit to the stablecoin issuer’s bank. Each action pushes down the supplementary leverage ratio. These structural bottlenecks create the possibility of price deviations, delayed redemptions, or runs—especially when redemption demand rises rapidly.

We next extended this analysis by showing that the *technological substrate* of stablecoins introduces a qualitatively different layer of risk. Smart-contract design, bridge and oracle architectures, validator incentives, governance structures, and the liveness of public blockchains all shape a stablecoins operational reliability. Failures in these components—whether from logic bugs, key mismanagement, consensus faults, or adversarial attacks—can impair users’ ability to transfer or redeem tokens even when backing assets remain intact. Moreover, the value transacted in stablecoins can itself amplify incentives to attack the underlying blockchain, creating a two-way linkage between financial scale and cyber vulnerability. These mechanisms illustrate that operational failures can propagate into financial instability through loss of confidence, impaired liquidity, or sudden redemption pressures.

Finally, we evaluated how the GENIUS regulatory framework addresses these risks—and where it does not. The Act succeeds in strengthening asset quality, transparency, and supervisory oversight. Its prohibition on rehypothecation of backing assets and its monthly public disclosures meaningfully reduce hidden leverage and opacity. Yet, key dilemmas remain unresolved. GENIUS appears to forbid explicitly the direct application of minimum bank-style capital requirements to issuers, even though they issue demandable liabilities vulnerable to run dynamics. It also leaves redemption mechanics undefined and does not address the liquidity bottlenecks created by dealer balance-sheet constraints. Most importantly, it does not resolve the policy dilemma outlined in Section 5.4: whether stablecoin issuers should have access to Federal Reserve liquidity facilities. Such access could materially improve resilience during stress but carries implications for the implementation of monetary policy and the banking system.

Taken together, our findings show that achieving durable stability in the stablecoin sector will require more than rules that delimit allowable backing assets. It will require an integrated approach that accounts for financial-market structure and blockchain-level risks. It requires careful consideration of the difference between a bank and a nonbank issuer of money-like claims. GENIUS provides a strong foundation, but further policy development—guided by the studies it mandates—will be necessary to ensure that stablecoins can function reliably as scalable, dollar-denominated payment instruments in both normal and stressed conditions.

10 Acknowledgements

We are grateful for the excellent research and analytical support provided by Jenny Jin and thank the following individuals for their insight, suggestions, and feedback: Pablo Azar, Robert Bench, Pavel Chichkanov, Eziechel Copic, Ethan Heilman, Tim Massad, Susan McLaughlin, and Madars Virza.

This work was supported by funding from the MITRE Corporation. The content, analyses, and conclusions presented in this report are those of the authors and do not necessarily reflect the views, positions, or policies of the MITRE Corporation or any affiliated organization.

References

- 12 U.S.C. § 5903. 2025. <https://www.law.cornell.edu/uscode/text/12/5903> Section (a)1(B).
- 12 U.S.C. §§ 5901–5916. 2025a. <https://www.congress.gov/119/plaws/publ27/PLAW-119publ27.pdf> Section 4(a)(1).
- 12 U.S.C. §§ 5901–5916. 2025b. <https://www.congress.gov/119/plaws/publ27/PLAW-119publ27.pdf> Section 4(c)(2).
- Gara Afonso, Marco Cipriani, Adam Copeland, Anna Kovner, Gabriele La Spada, and Antoine Martin. 2021. The Market Events of Mid-September 2019. Economic Policy Review 27, 2 (August 2021). https://www.newyorkfed.org/research/epr/2021/epr_2021_market-events_afonso JEL classification: E42, E58, G14.
- Rashad Ahmed and Iñaki Aldasoro. 2025. Stablecoins and Safe Asset Prices. BIS Working Paper 1270. Bank for International Settlements. <https://www.bis.org/publ/work1270.htm>
- Kyle D. Allen and Drew B. Winters. 2020. Crisis regulations: The unexpected consequences of floating NAV for money market funds. Journal of Banking & Finance 117 (2020), 105851. <https://doi.org/10.1016/j.jbankfin.2020.105851>
- Kenechukwu Anadu, Pablo Azar, Marco Cipriani, Thomas M. Eisenbach, Catherine Huang, Mattia Landoni, Gabriele La Spada, Marco Macchiavelli, Antoine Malfroy-Camine, and J. Christina Wang. 2024. Runs and Flights to Safety: Are Stablecoins the New Money Market Funds? Staff Report 1073. Federal Reserve Bank of New York. https://www.newyorkfed.org/research/staff_reports/sr1073.html
- Sriya Anbil, Alyssa G. Anderson, and Zeynep Senyuz. 2020. What Happened in Money Markets in September 2019? FEDS Notes 2020-02-27. Board of Governors of the Federal Reserve System. <https://doi.org/10.17016/2380-7172.2527>
- Robert Armstrong. 2025. Stablecoins are Bank Deposits. Financial Times (27 May 2025). <https://www.ft.com/content/625f9f0e-0144-4bc4-99e2-571ab64ccbe9>
- Daniel Aronoff, Sriram Rajan, and Madars Virza. 2026. An Empirical Decomposition and Analysis of the US Treasuries Repo Market. (2026). Forthcoming.

- Daniel J. Aronoff, Robert M. Townsend, and Madars Virza. 2025. RepoMech: A Method to Reduce the Balance-Sheet Impact of Repo Intermediation. arXiv:2512.23842 [econ.GN] <https://arxiv.org/abs/2512.23842>
- Bank for International Settlements. 2010. Basel III: A global regulatory framework for more resilient banks and banking systems. Technical Report. Bank for International Settlements. <https://www.bis.org/publ/bcbs189.pdf>
- Bank of England. 2025a. Proposed Regulatory Regime for Sterling-Denominated Systemic Stablecoins. Consultation Paper CP. Bank of England. <https://www.bankofengland.co.uk/paper/2025/cp/proposed-regulatory-regime-for-sterling-denominated-systemic-stablecoins> Consultation paper outlining the Bank's proposed regime for systemic stablecoins in the UK.
- Bank of England. 2025b. Proposed regulatory regime for sterling-denominated systemic stablecoins. <https://www.bankofengland.co.uk/paper/2025/cp/proposed-regulatory-regime-for-sterling-denominated-systemic-stablecoins>
- BNB Chain Team. 2022. BNB Chain Ecosystem Update. BNB Chain Blog. <https://www.bnbchain.org/en/blog/bnb-chain-ecosystem-update>
- Board of Governors of the Federal Reserve System. 2021. Standing Overnight Repurchase Agreement Facility. <https://www.federalreserve.gov/monetarypolicy/standing-overnight-repurchase-agreement-facility.htm>. Accessed: 2025-12-10.
- Board of Governors of the Federal Reserve System. 2024. Financial Accounts of the United States. <https://www.federalreserve.gov/releases/z1/release-dates.htm> Z.1 release.
- David Bowman, Yesol Huh, and Sebastian Infante. 2024. Balance-Sheet Netting in U.S. Treasury Markets and Central Clearing. Finance and Economics Discussion Series 2024-057. Board of Governors of the Federal Reserve System, Washington, D.C. <https://doi.org/10.17016/FEDS.2024.057>
- Vitalik Buterin. 2016. CRITICAL UPDATE Re: DAO Vulnerability. Ethereum Foundation Blog. <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability>
- Nic Carter. 2025. The Last Word on Stablecoins and Free Banking. [https://murmurationstwo.substack.com/p/the-last-word-on-stablecoins-and](https://murmurationstwo.substack.com/p/the-last-word-on-stablecoins-and-murmurationstwo) Murmurationstwo Substack.
- CertiK. 2022. Wormhole Bridge Exploit Incident Analysis. CertiK Blog. <https://www.certik.com/resources/blog/wormhole-bridge-exploit-incident-analysis>
- Circle. 2025. <https://investor.circle.com/financials/quarterly-results/default.aspx>

- Citi Institute, Global Perspectives & Solutions. 2025. Stablecoins 2030: Web3 to Wall Street. Technical Report. Citigroup. https://www.citigroup.com/rcs/citigpa/storage/public/GPS_Report_Stablecoins_2030.pdf Base-case forecast: US\$1.9 trillion by 2030; Bull-case: US\$4.0 trillion.
- Coinbase. 2019. Deep Chain Reorganization Detected on Ethereum Classic (ETC). Coinbase Blog. <https://www.coinbase.com/blog/deep-chain-reorganization-detected-on-ethereum-classic-etc>
- Committee on Capital Markets Regulation. 2021. The U.S. Treasury Market During the COVID-19 Crisis. Technical Report. Committee on Capital Markets Regulation. <https://capmktreg.org/wp-content/uploads/2022/12/NBTF-US-Treasury-Markets-During-Covid-2.pdf> PDF report.
- Committee on Payments and Market Infrastructures. 2023. Considerations for the use of stablecoin arrangements in cross-border payments. Technical Report. Bank for International Settlements. <https://www.bis.org/cpmi/publ/d220.pdf>
- Adam Copeland, Darrell Duffie, and Yilin Yang. 2021. Reserves Were Not So Ample After All. NBER Working Paper 29090. National Bureau of Economic Research. <https://doi.org/10.3386/w29090>
- Tri Vi Dang, Gary Gorton, Bengt Holmström, and Guillermo Ordoñez. 2017. Banks as Secret Keepers. American Economic Review 107, 4 (2017), 1005–1029. <https://doi.org/10.1257/aer.20140782>
- Chuan Du, Ria Sonawane, and Cy Watsky. 2025. In the Shadow of Bank Runs: Lessons from the Silicon Valley Bank Failure and Its Impact on Stablecoins. FEDS Notes, Board of Governors of the Federal Reserve System. <https://www.federalreserve.gov/econres/notes/feds-notes/in-the-shadow-of-bank-run-lessons-from-the-silicon-valley-bank-failure-and-its-impact-on-stablecoins-20251217.html>
- Darrell Duffie. 2017. Post-Crisis Bank Regulations and Financial Market Liquidity. Technical Report. Banca d'Italia. <https://www.bancaditalia.it/pubblicazioni/lezioni-baffi/lecture-13/index.html> Tredicesima Lezione Paolo Baffi di Moneta e Finanza.
- Darrell Duffie, Michael Fleming, Frank Keane, Albert Kyle, and Jonathan McCormick. 2021. The U.S. Treasury Market during the COVID-19 Crisis. Discussion Paper. Program on International Financial Systems / Brookings (New Bond Trade Forum). <https://capmktreg.org/wp-content/uploads/2022/12/NBTF-US-Treasury-Markets-During-Covid-2.pdf>

- Darrell Duffie and Donald R. Wilson. 2025. The case for a new floating rate Treasury note. <https://www.brookings.edu/articles/the-case-for-a-new-floating-rate-treasury-note/> Commentary / Op-ed, Economic Studies (Hutchins Center on Fiscal and Monetary Policy).
- Marc Farag, Damian Harland, and Dan Nixon. 2013. Bank capital and liquidity. Bank of England Quarterly Bulletin 2013 Q3 (2013). <https://www.bankofengland.co.uk/-/media/boe/files/quarterly-bulletin/2013/bank-capital-and-liquidity>
- Federal Deposit Insurance Corporation. 2022. Formal and Informal Enforcement Actions Manual. <https://www.fdic.gov/regulations/examinations/enforcement-actions/ch-05.pdf> Chapter 5.
- Federal Reserve. 2025. <https://www.federalreserve.gov/newsevents/speech/waller20251021a.htm> Accessed: 2025-12-23.
- FFIEC. 2025. https://www.ffiec.gov/sites/default/files/data/reporting-forms/FFIEC031_FFIEC041_202503_i.pdf
- Michael J. Fleming, Frank M. Keane, and Ernst Schaumburg. 2016. Primary Dealer Participation in the Secondary U.S. Treasury Market. Liberty Street Economics, Federal Reserve Bank of New York (Feb. 2016). <https://libertystreeteconomics.newyorkfed.org/2016/02/primary-dealer-participation-in-the-secondary-us-treasury-market/>
- Michael J. Fleming, Haoyang Liu, Rich Podjasek, and Jake Schurmeier. 2022. The Federal Reserve's Market Functioning Purchases. Economic Policy Review 28, 1 (June 2022), 210–241. https://www.newyorkfed.org/medialibrary/media/research/epr/2022/epr_2022_mfp_fleming.pdf Federal Reserve Bank of New York.
- Michael J. Fleming and Francisco Ruela. 2020. Treasury Market Liquidity during the COVID-19 Crisis. Liberty Street Economics (17 April 2020). <https://libertystreeteconomics.newyorkfed.org/2020/04/treasury-market-liquidity-during-the-covid-19-crisis/>
- Charles A. E. Goodhart. 1988. The Evolution of Monetary Institutions. In The Evolution of Monetary Institutions: Money and Credit in the Light of Economic Theory. MIT Press.
- Gary Gorton and Jeffery Zhang. 2023. Taming Wildcat Stablecoins. The University of Chicago Law Review (2023). <https://chicagounbound.uchicago.edu/uclrev/vol90/iss3/3/>
- Valentin Haddad, Alan Moreira, and Tyler Muir. 2021. When Selling Becomes Viral: Disruptions in Debt Markets in the COVID-19 Crisis. The Review of Financial Studies 34, 11 (2021), 5309–5351. <https://doi.org/10.1093/rfs/hhab040>

- Samuel J. Hempel, Calvin Isley, R. Jay Kahn, and Patrick E. McCabe. 2023a. Money Market Fund Repo and the ON RRP Facility. FEDS Notes. Board of Governors of the Federal Reserve System, Washington, DC. <https://doi.org/10.17016/2380-7172.3412>
- Samuel J. Hempel, R. Jay Kahn, Robert Mann, and Mark E. Paddrik. 2023b. Why Is So Much Repo Not Centrally Cleared?: Lessons from a Pilot Survey of Non-centrally Cleared Repo Data. OFR Brief Series 23-01. Office of Financial Research, U.S. Department of the Treasury, Washington, DC. https://www.financialresearch.gov/briefs/files/OFRBrief_23-01_Why-Is-So-Much-Repo-Not-Centrally-Cleared.pdf
- Samuel J. Hempel, R. Jay Kahn, and Julia Shephard. 2025. The \$12 Trillion US Repo Market: Evidence from a Novel Panel of Intermediaries. FEDS Notes (July 11 2025).
- Bengt Holmström. 2015. Banks as Secret Keepers. Technical Report 479. Bank for International Settlements. <https://www.bis.org/publ/work479.pdf>
- Bengt Holmström and Jean Tirole. 1998. Private and Public Supply of Liquidity. Journal of Political Economy 106, 1 (1998), 1–40.
- Vicky Ge Huang, Hannah Miao, and Caitlin Ostroff. 2023. Circle’s USDC Stablecoin Breaks Peg With \$3.3 Billion Stuck at Silicon Valley Bank. Wall Street Journal (11 March 2023). <https://www.wsj.com/articles/crypto-investors-cash-out-2-billion-in-usd-coin-after-bank-collapse-1338a80f>
- Inter-Agency Working Group on Treasury Market Surveillance. 2021. Recent Disruptions and Potential Reforms in the U.S. Treasury Market: A Staff Progress Report. Technical Report. U.S. Department of the Treasury; Board of Governors of the Federal Reserve System; Federal Reserve Bank of New York; Securities and Exchange Commission; Commodity Futures Trading Commission. <https://home.treasury.gov/system/files/136/IAWG-Treasury-Report.pdf> PDF report.
- J.M. Keynes. 1930. A Treatise on Money. Number v. 2 in A Treatise on Money. Harcourt, Brace. <https://books.google.com/books?id=qAq8AAAAIAAJ>
- János Kornai, Eric Maskin, and Gérard Roland. 2003. Understanding the Soft Budget Constraint. Journal of Economic Literature 41, 4 (2003), 1095–1136. <https://doi.org/10.1257/002205103771799999>
- Paul R. Krugman, Maurice Obstfeld, and Marc J. Melitz. 2012. International Economics: Theory and Policy (9 ed.). Pearson, Boston.
- Leland Lee and Haseeb Qureshi. 2019. Ethereum Is Now Unforkable, Thanks to DeFi. Dragonfly Research. <https://medium.com/dragonfly-research/ethereum-is-now-unforkable-thanks-to-defi-9818b967738f> Medium article.

- Nellie Liang. 2025a. Stablecoins: Issues for regulators as they implement GENIUS Act. <https://www.brookings.edu/articles/stablecoins-issues-for-regulators-as-they-implement-genius-act/> Brookings Institute.
- Nellie Liang. 2025b. Testimony on U.S. Treasury Market Resilience and its Importance. Hearing on “U.S. Treasury Debt in the Monetary System,” House Financial Services Committee, 119th Congress. <http://docs.house.gov/meetings/BA/BA00/20250408/118116/HHRG-119-BA00-Wstate-LiangN-20250408.pdf> Written testimony, showing U.S. Treasury market daily volumes and liquidity.
- Jiageng Liu, Igor Makarov, and Antoinette Schoar. 2023. Anatomy of a Run: The Terra Luna Crash. Working Paper 31160. National Bureau of Economic Research. <http://www.nber.org/papers/w31160> NBER Working Paper No. 31160.
- Yiming Ma, Yao Zeng, and Anthony Lee Zhang. 2025. Stablecoin Runs and the Centralization of Arbitrage. <https://bfi.uchicago.edu/insights/stablecoin-runs-and-the-centralization-of-arbitrage/>
- Perry Mehrling. 2013. The Inherent Hierarchy of Money. In Social Fairness and Economics: Economic Essays in the Spirit of Duncan Foley, Lance Taylor, Armon Rezai, and Thomas Michl (Eds.). Routledge, London & New York, 394–404. https://sites.bu.edu/perry/files/2019/04/Mehrling_P_FESeminar_Sp12-02.pdf Prepared January 25, 2012 for the Duncan Foley Festschrift volume and conference April 20–21, 2012.
- Frederic S. Mishkin. 2019. The Economics of Money, Banking, and Financial Markets (12 ed.). Pearson, Boston.
- Neha Narula. 2021. The Technology Underlying Stablecoins. <https://nehanarula.org/2021/09/23/stablecoins.html> Blog post on Neha’s Writings.
- Joachim Neu, Ertem Nusret Tas, and David Tse. 2020. A Balancing Attack on Gasper, the Current Candidate for Eth2’s Beacon Chain. ETH Research Forum. <https://ethresear.ch/t/a-balancing-attack-on-gasper-the-current-candidate-for-eth2s-beacon-chain/8079>
- Michael Neuder, Daniel Moroz, R. Rao, and David Parkes. 2021. Low-Cost Attacks on Ethereum 2.0 by Sub-1/3 Stakeholders. arXiv preprint arXiv:2102.02247. <https://arxiv.org/abs/2102.02247>
- NIST. 2025. Post-Quantum Cryptography. <https://www.nist.gov/pqcrypto> Accessed: 2025-12-23.
- Congressional Budget Office. 2025. The Long-Term Budget Outlook: 2025 to 2055. Technical Report. Congressional Budget Office. <https://www.cbo.gov/publication/61270>

- Mark E. Paddrik, Robert J. Kahn, Matthew McCormick, and Vy Nguyen. 2023. Anatomy of the Repo Rate Spikes in September 2019. Working Paper 23-04. Office of Financial Research. <https://www.financialresearch.gov/working-papers/2023/04/25/anatomy-of-the-repo-rate-spikes-in-september-2019/>
- Mark E. Paddrik, Carlos A. Ramírez, and Matthew J. McCormick. 2021. The Dynamics of the U.S. Overnight Triparty Repo Market. FEDS Notes. Board of Governors of the Federal Reserve System, Washington, DC. <https://doi.org/10.17016/2380-7172.2948>
- Nikhil Kumar Parida, Chandrashekar Jatoth, V. Dinesh Reddy, Md. Muzakkir Hussain, and Jamilurahman Faizi. 2023. Post-quantum distributed ledger technology: a systematic survey. *Nature: Scientific Reports*. <https://www.nature.com/articles/s41598-023-47331-1>
- Paxos. 2025a. <https://www.paxos.com/pyusd-transparency#pyusd-attestations>
- Paxos. 2025b. <https://www.paxos.com/usdp-transparency>
- Jerome H. Powell. 2025. Speech by Chair Powell on the economic outlook and monetary policy. <https://www.federalreserve.gov/newsevents/speech/powell20251014a.htm>. Accessed: 2025-12-10.
- Ripple. 2025. <https://ripple.com/solutions/stablecoin/transparency/>
- Ronin Network. 2022. Community Alert: Ronin Validators Compromised. Ronin Blog. <https://roninchain.com/blog/posts/community-alert-ronin-validators-6513cc78a5edc1001b03c366>
- David Salerno, John A. Ruddy, and Murl Rajan. 2016. Changes to Accounting for Repurchase Agreements. The CPA Journal (August 2016). <https://www.cpajournal.com/2016/08/01/changes-accounting-repurchase-agreements/>
- Caspar Schwarz-Schilling, Joachim Neu, Barnabé Monnot, Aditya Asgaonkar, Ertem Nusret Tas, and David Tse. 2021. Three Attacks on Proof-of-Stake Ethereum. arXiv preprint. <https://arxiv.org/abs/2110.10086>
- Securities and Exchange Commission. 2023. Standards for Covered Clearing Agencies for U.S. Treasury Securities and Application of the Broker-Dealer Customer Protection Rule With Respect to U.S. Treasury Securities. Technical Report. Securities and Exchange Commission. <https://www.sec.gov/files/rules/final/2023/34-99149.pdf> 17 CFR Part 240, [Release No. 34-99149; File No. S7-23-22] RIN 3235-AN09.
- Hyun Song Shin. 2025. The next-generation monetary and financial system. In 2025 Annual Economic Report, Bank for International Settlements (Ed.). Bank for International Settlements, Basel, Chapter III. <https://www.bis.org/publ/arpdf/ar2025e3.htm>

- Sullivan & Cromwell LLP. 2025. S&C Memo: Stablecoin Legislation. https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/Stablecoin-Legislation.pdf p. 4.
- Tether. 2025. https://assets.ctfassets.net/vyse88cgwfb1/2SGAAXnsblwKByIzkhcbSx/9efa4682b3cd4c62d87a4c88ee729693/ISAE_3000R_-_Opinion_Tether_International_Financial_Figure_RC187322025BD0201.pdf
- Tether. 2025. Tether Unveils USAT, its Planned U.S.-Regulated Dollar-Backed Stablecoin, and Will Appoint Bo Hines as CEO of Tether USAT. <https://tether.io/news/tether-unveils-usat-its-planned-u-s-regulated-dollar-backed-stablecoin-and-will-appoint-bo-hines-as-ceo-of-tether-usat/>
- Tether. 2025. Tether Unveils USAT, its Planned U.S.-Regulated Dollar-Backed Stablecoin, and Will Appoint Bo Hines as CEO of Tether USAT. <https://tether.io/news/tether-unveils-usat-its-planned-u-s-regulated-dollar-backed-stablecoin-and-will-appoint-bo-hines-as-ceo-of-tether-usat/>
- Uniswap. 2025. <https://app.uniswap.org/explore/tokens/ethereum/0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48> Accessed: 2025-12-23.
- U.S. Government Accountability Office. 2023. Money Market Mutual Funds: Pandemic Revealed Unresolved Vulnerabilities. Technical Report GAO-23-105525. U.S. Government Accountability Office. <https://www.gao.gov/assets/gao-23-105535.pdf>
- U.S. Government Accountability Office. 2024. Bank Supervision: More Timely Escalation of Supervisory Action Needed. Technical Report GAO-24-106974. U.S. Government Accountability Office. <https://www.gao.gov/assets/870/866411.pdf>
- U.S. Securities and Exchange Commission. [n. d.]. Money Market Fund Reform; Amendments to Form PF. Final rule release. <https://www.sec.gov/files/rules/final/2014/33-9616.pdf> File No. S7-03-13; Federal Register citation: 79 FR 47735 (Aug. 14, 2014); effective Oct. 14, 2014.
- U.S. Securities and Exchange Commission. 2017. Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. Technical Report Release No. 81207. U.S. Securities and Exchange Commission. <https://www.sec.gov/files/litigation/investreport/34-81207.pdf>
- Dimitri Vayanos and Jean-Luc Vila. 2021. A Preferred-Habitat Model of the Term Structure of Interest Rates. Econometrica 89, 1 (2021), 77–112.

A Appendix: Leverage Ratio Calculations

In Section 4, we analyzed the capitalization of select stablecoin issuers using a capital measure applied by U.S. bank regulators: the leverage ratio. We found sufficient data in public filings from five prominent stablecoin issuers to calculate a simplified version of the most fundamental capital requirement for commercial banks, the minimum leverage ratio, for periods ranging from three to ten recent quarters.

To calculate the leverage ratio, we applied the requirements set out in the Federal Financial Institutions Examination Council’s “Instructions for Preparation of Consolidated Reports of Condition and Income, FFIEC 031 and FFIEC 041” as of March 2025, Section RC-R (FFIEC, 2025). We made assumptions about the stablecoin issuers’ data to fit that data into the Basel III leverage ratio standards. For example, we assumed that the U.S. Treasuries and the securities that the five stablecoin issuers reporting purchasing from a third party under an agreement to resell (“reverse repos”) would qualify under the GENIUS Act as acceptable reserve assets, even though regulators have not yet defined the requirements.

We moreover made simplifying assumptions about the form of the stablecoin issuers’ capital. As defined by the Basel III and the FFIEC filing instructions, Tier 1 capital has two components: Common Equity Tier 1 (CET1) and Additional Tier 1 capital (AT1). This latter category consists of common shares and stock surplus, retained earnings, other comprehensive income, qualifying minority interest and regulatory adjustments. Given the unspecified structure of stablecoin issuers’ capital, we assumed that all equity (total value of reserve assets - total value of coins in circulation) that each stablecoin issuer reported consists solely of Tier 1 capital. We furthermore assumed that the issuer’s total assets are equal to the total value of all reserve backing assets.

With those assumptions in hand, we then calculated a simplified version of the Basel leverage ratio using the following formula:

$$\text{Leverage Ratio} = \frac{\text{Total Value of the Reserve Assets} - \text{Total Value of the Coins in Circulation}}{\text{Total Value of the Reserve Assets}}$$

Higher ratios indicate that more capital is available to support a bank’s unweighted assets, thereby strengthening the bank’s ability to absorb unexpected losses from any source and improving its resilience. Under the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA), U.S. commercial banks must have leverage ratios of at least 4% to meet minimum requirements to be considered adequately capitalized and at least 5% to be considered “well-capitalized.” (This latter and most favorable designation was meant to indicate that the risk of failure is low.)

Commercial banks with leverage ratios below 4% are considered undercapitalized. This unfavorable designation deteriorates to “significantly undercapitalized” below 3% and “critically undercapitalized” at less than 2%. Under FDICIA’s “prompt corrective action” rules, U.S. bank regulators typically must close critically undercapitalized banks and put them into receivership within 90 days, setting clear expectations for

regulatory intervention (Federal Deposit Insurance Corporation, 2022; U.S. Government Accountability Office, 2024). Stablecoin issuers lack such safeguards at present.

Three of the issuers we studied, namely Circle, PayPal, and Paxos, reported reserve assets that consist primarily of cash, deposits, and U.S. Treasury-related securities, including reverse repos; as such, these three issuers appear to conform to the limitations set by the GENIUS Act on reserve assets that regulated payment stablecoin issuers are permitted to hold. We cannot confirm that these reserve assets qualify, especially since regulators have not yet defined these steps. The other two issuers, namely Tether and Ripple, held assets such as corporate bonds or even digital assets such as Bitcoin; as such, these two issuers would not meet the requirements set out in the GENIUS Act.

As indicated in Table 2, none of the three firms whose reserve assets appear to conform to the GENIUS Act's requirements would have been considered adequately capitalized under the leverage ratio requirement for commercial banks over the entire period we studied. Two of the three would have been considered critically undercapitalized in all quarters for which they provided data, and the third would have declined from significantly undercapitalized to critically undercapitalized in the most recent two quarters.

In contrast, Tether met the minimum 4% leverage requirement in five quarters and would have been considered "well capitalized" (above 5%) in two of those five quarters. The remaining issuer, Ripple, met the minimum requirement in two quarters, of which one quarter it was well-capitalized using this one measure of capital.

However, since these leverage ratios predate the GENIUS Act, these ratios reflect the inclusion of some higher-risk assets that historically have not maintained stable value, such as corporate bonds, and volatile digital assets, such as Bitcoin, included in Tether's reserve assets. In fact, as of the second quarter of 2025, Bitcoin was equivalent to nearly 5.5% of its total assets; if the value of Bitcoin were to drop to zero, Tether's liabilities would exceed its assets, rendering it insolvent on paper. As mentioned earlier, Tether has announced plans to introduce a new U.S. dollar-based digital asset, USAT, that will comply with the GENIUS Act's limitations on the kinds of permissible reserve assets it may hold, but this coin has not been issued at the time of this writing. (Tether, 2025).

B Attacks on blockchains

Table 5: Major Blockchain Attacks: Technical Cause, Value, and Price Reaction

Sources: (Buterin, 2016; U.S. Securities and Exchange Commission, 2017; Ronin Network, 2022; CertiK, 2022; BNB Chain Team, 2022; Coinbase, 2019).

Incident (year)	Main chain / token(s)	Nature of attack	Est. value stolen / created (USD, at time)	Approx. immediate price response
The DAO hack (Buterin 2016, SEC 2017)	Ethereum / ETH	Smart-contract bug (reentrancy / recursive calls) in The DAO contract, allowing repeated withdrawals before balances updated.	About 3.6 million ETH; \$50–\$60M at the time.	ETH \$21.50 → \$15 within hours (~ 30% intraday).
Ronin bridge hack (Ronin Network 2022)	Ronin / RON; Axie Infinity / AXS	Cross-chain bridge validator key compromise; attacker controlled 5/9 validators and forged withdrawals.	173,600 ETH + 25.5M USDC (~ \$540–\$620M).	RON down ~ 20–22% in 24h; AXS \$70 → \$64.3 (~ 8%).
Wormhole bridge exploit (CertiK blog 2022)	Solana / SOL (Wormhole bridge)	Bridge smart-contract vulnerability on Solana; attacker bypassed verification checks and minted 120k wETH.	About 120,000 wETH (~ \$320–\$326M).	SOL \$111 → \$96 in 24h (~ 13.5%).
BNB Chain bridge hack (BNB 2022)	BNB Chain / BNB	Cross-chain bridge exploit on BSC Token Hub; forged proof/messages enabled unauthorized withdrawal of ~2,000,000 BNB.	~ \$570M (only ~ \$100M bridged out).	BNB down ~ 3.5% over 24h, to ~ \$281 after disclosure.
Ethereum Classic 51% attack (Coinbase 2019)	Ethereum Classic / ETC	51% / majority-hashpower attack; deep reorgs and double-spends of exchange deposits.	About 219,500 ETC double-spent (~ \$1.1M).	ETC from ~ \$5.51 (24h high) to ~ \$4.93 (low); > 7.5% daily loss, > 10% from high.

Notes: Figures are approximate and refer to conditions at the time of each incident. “Immediate price response” is the first intraday / 24-hour reaction after public disclosure.