

Considerations for the Regulation of Algorithmic Stablecoins

a16z Crypto Policy Team*

March 2023

*Founded in Silicon Valley in 2009 by Marc Andreessen and Ben Horowitz, Andreessen Horowitz, known as "a16z," is a venture capital firm that backs entrepreneurs building the future through technology. a16z Crypto is an a16z fund that invests in crypto and web3 startups. The a16z crypto policy team works with founders, lawmakers, and regulators around the globe to help shape the legislation that will govern the future of web3.

Executive Summary

Roughly six years after the publication of Satoshi Nakamoto’s Bitcoin whitepaper, the world’s first stable-value cryptocurrency or “stablecoin” was launched.¹ Stablecoins are intended to address the issue of price volatility amongst many cryptocurrencies and to provide a reliable, blockchain-enabled means of exchange. To accomplish this, stablecoins attempt to peg their value to a reference asset—typically a fiat currency or other exchange-traded commodity. This in turn allows users to both transact with one another through borderless, decentralized blockchain protocols all the while relying on the low volatility and dependability of the associated fiat currency, such as the U.S. dollar. Since 2014, the number of stablecoins in circulation has proliferated, and the total market capitalization of stablecoins has surpassed well over \$100 billion.² Stablecoins have become deeply embedded throughout the web3 ecosystem, and play an important role in the next generation of democratized financial services.³ Moreover, stablecoins support other, innovative, non-financial services by facilitating a blockchain-enabled method of value transfer.

Today’s stablecoins employ a wide variety of mechanisms to stabilize their value. For example, the largest stablecoins by market capitalization, USD Coin and Tether,⁴ attempt to peg their value to the U.S. dollar on an approximately one-to-one basis by primarily holding reserves of traditional financial assets (*e.g.*, cash, treasury bills, fiduciary deposits, commercial paper, etc.) in trust at regulated financial institutions. Other stablecoins—often referred to as algorithmic stablecoins—may rely on digital assets as collateral and employ algorithms to liquidate collateral as needed. For purposes of this paper, we define “algorithmic stablecoins” as cryptocurrencies that (i) peg their value to a fiat currency, (ii) are collateralized by digital assets such as crypto tokens, and (iii) are governed by algorithms that are designed to dynamically ensure adequate levels of collateral and reduce the price volatility of such stablecoin.

The widely reported crash of one poorly designed algorithmic stablecoin, TerraUSD (“UST”), has renewed interest in regulating stablecoins.⁵ Against this backdrop, it is important that legislators and regulators understand the details of what happened and the nuance of the ecosystem in order to ultimately develop and apply measured and thoughtful new regulations to stablecoins. America’s technological and financial edge has always depended on business leaders and policymakers collaborating to ensure that the private sector can experiment and build, while appropriate regulatory regimes mitigate the real downside risks that might otherwise harm consumers. Along with stablecoin technology, smart and effective stablecoin regulation will be critical in protecting consumers, preventing financial crime, and preserving the safety and stability of the financial system. However, many proposals have reflexively gone too far—with some proposing what would be an effective ban on all algorithmic stablecoins. For example, California’s previously proposed legislative bill, AB 2269, would have prohibited stablecoin issuances from issuers other than

¹ Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. <https://bitcoin.org/bitcoin.pdf>. <https://blog.bitmex.com/wp-content/uploads/2018/06/173481633-BitShares-White-Paper.pdf>.

² Hoskinson, C., Larimer, D., and Larimer, S. (2014). *BitShares A Peer-to-Peer Polymorphic Digital Asset Exchange (P2P-PDAE)*. <https://coinmarketcap.com/view/stablecoin/>.

³ A strong majority of crypto asset trades today involve a stablecoin. <https://www.theblockcrypto.com/data/crypto-markets/spot>.

⁴ <https://tether.to/en/transparency/#reports>; <https://www.circle.com/en/usdc#transparency>.

⁵ Genc, E. and Sandor, K. (2022). “The Fall of Terra: A Timeline of the Meteoric Rise and Crash of UST and Luna,” *Coindesk*. <https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/>.

licensed banks or institutions that maintain limited types of non-digital collateral in excess of the value of the stablecoins issued. As discussed below, such a ban would have had a number of negative and unintended secondary effects, including harming the very consumers it was intended to protect.

We posit that policymakers should focus on four core principles when considering regulation for algorithmic stablecoins: (1) protecting consumers and advancing equitable access; (2) ensuring the integrity of issuers and reserves; (3) strengthening the technological and operational resilience of stablecoin networks; and (4) ensuring that the U.S. dollar remains the reserve currency of the internet. In particular, there are seven considerations policymakers should take into account where stablecoin regulation is concerned:

- 1. Stablecoin regulations should not treat all stablecoins as though they are the same.** Stablecoin regulations should recognize the diversity of stablecoin designs and be calibrated to each design's specific risks.
- 2. Stablecoin regulations should be designed to keep innovation onshore.** Regulation that fails to accommodate algorithmic stablecoins could accelerate the U.S.'s declining market share of web3 developers and hinder its ability to influence web3's development.
- 3. Stablecoin regulations should be designed to facilitate the propagation of U.S.-dollar-denominated stablecoins.** Regulations that do not address a wide range of stablecoin designs could lead to the propagation of non-dollar-denominated algorithmic stablecoins offshore, thereby jeopardizing the U.S. dollar's role as the reserve currency of the internet and threatening national security.
- 4. Stablecoin regulations should limit significant financial market disruption and user losses.** Reactive stablecoin regulations could have negative consequences from both an investor protection and software development perspectives, potentially resulting in billions of dollars of losses for the users that policymakers are trying to protect.
- 5. Stablecoin regulations should not unnecessarily impede technological development.** The algorithmic mechanisms utilized by algorithmic stablecoin protocols are prevalent across the decentralized finance ("DeFi") ecosystem and web3 industry more broadly. Accordingly, a broad-based regulatory attack on algorithmic stablecoins could inadvertently hinder a wide array of web3 innovation.
- 6. Stablecoin regulations must not be impractical or counterproductive to enforce.** Practically speaking, the U.S. could not remove all algorithmic stablecoins from its market. Overly restrictive regulations are therefore likely to encourage regulatory arbitrage, putting users at greater risk of harm.
- 7. Sensible regulatory options exist.** Regulators could have used existing regulations to prevent much of the recent harm throughout the web3 ecosystem, including the fall of UST. And more precise regulation could foster innovation and eliminate the risk of such systemic harm being repeated.

I. Not all stablecoins are the same.

As previously mentioned, the numerous stablecoins that exist today experiment with a variety of mechanisms to stabilize their value. The primary features that distinguish some algorithmic stablecoins

from others are: (1) the algorithms used by the stablecoin, and (2) the collateralization of the stablecoin. Generally speaking, stablecoins do not fail as a result of the use of an algorithm, but rather due to collateral design.

When a user mints (*i.e.*, receives) an algorithmic stablecoin, that user must nearly always deposit collateral with the stablecoin’s protocol. Almost all stablecoin protocols that use algorithms liquidate the user’s collateral deposit automatically if the value of the user’s outstanding stablecoins exceeds the value of the deposited collateral. This “Liquidation Amount” varies by stablecoin and is based on a collateralization ratio that its protocol establishes.

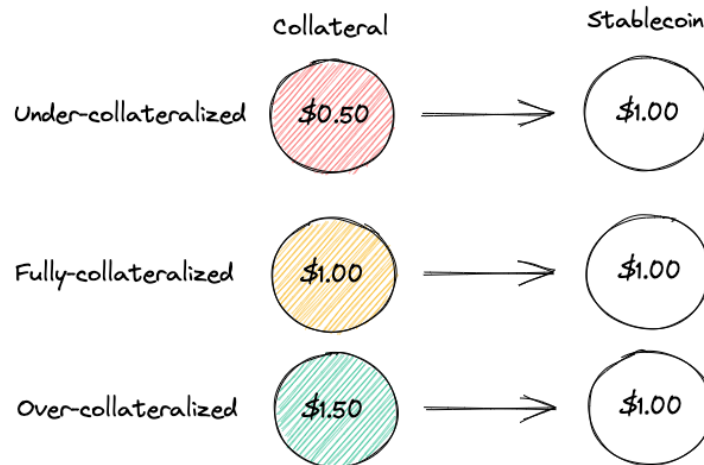
Many stablecoin protocols also seek to maintain their stablecoin’s peg through the use of algorithms that automatically incentivize minting or redemptions of stablecoins. These types of algorithmic stablecoins are widely used, and they have handled unprecedented redemptions while maintaining price stability throughout the most recent spikes of market volatility—both within the crypto ecosystem and the broader economy.^{6,7} Rather, what differentiates the risk with respect to particular algorithmic stablecoins is the collateralization required by the protocol to support the price of the stablecoin.

A stablecoin’s collateralization can be thought of as a function of two variables: (A) how much collateral a stablecoin protocol requires to mint a stablecoin and (B) what type of collateral market participants can deposit with the stablecoin protocol. The amount of collateral that a stablecoin protocol requires generally falls into three categories:

- **Under-collateralized** stablecoin protocols require less than \$1 of collateral to mint \$1 of stablecoins. Naturally, under-collateralized stablecoins are the most risky, as such a protocol would never have sufficient collateral to redeem all outstanding stablecoins. As a result, a “bank run” (*i.e.*, significant stablecoin redemptions), even without collateral price volatility, could result in a collapse.
- **Fully-collateralized** stablecoin protocols require exactly \$1 of collateral to mint \$1 of stablecoin. For fully-collateralized stablecoins, any price volatility with respect to the deposited collateral will likely result in such stablecoins becoming under-collateralized and therefore subject to the same risks as under-collateralized stablecoins.
- **Over-collateralized** stablecoin protocols require more than \$1 of collateral to mint \$1 of stablecoins. Over-collateralized stablecoins are the least risky. So long as the liquidation algorithms for such stablecoins function properly, they should ensure that the protocol always maintains more than \$1 of collateral for every \$1 of outstanding stablecoins. As a result, stablecoin holders can always redeem their stablecoins for \$1 of collateral.

⁶ <https://www.coinbase.com/price/dai>

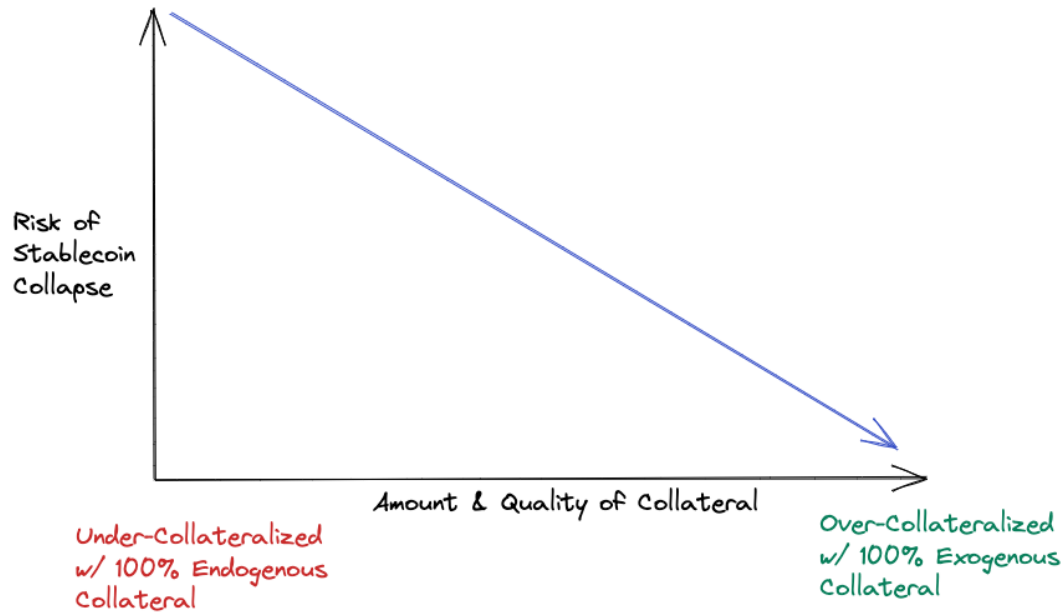
⁷ <https://www.coinbase.com/price/frax>



The type or quality of collateral supporting an algorithmic stablecoin can fall into two categories:

- **Endogenous collateral** consists of digital collateral that is native to the issuing protocol and whose value is dependent on the success/failure of the stablecoin protocol. For example, the collateral supporting UST’s peg to the U.S. dollar largely consisted of LUNA, the native governance token of the Terra Protocol on which UST was minted. Using endogenous collateral is risky as “bank runs” result in the value of the collateral declining, thereby leading to further redemptions. Stablecoins utilizing endogenous collateral are also particularly dangerous because they are capable of explosive growth. As a protocol’s native governance token increases in value, users holding the native governance token can mint more stablecoins with no external cost, and the reflexive relationship compounds. But when the price of the native governance token declines after such explosive growth, the resultant bank runs can be disastrous.
- **Exogenous collateral** consists of collateral external to the issuing system and whose value is not dependent on the success or failure of the stablecoin protocol (e.g., where a stablecoin protocol uses Bitcoin (“BTC”) and Ether (“ETH”) as collateral for the issuance of its stablecoin). Exogenous collateral is far less risky compared to endogenous collateral because a decline in the use or value of the protocol has no direct impact on the value of the collateral. Therefore, redemptions (which can cause a “bank run” in systems with endogenous collateral) do not trigger a decline in the value of the collateral and the system stays resilient.

Combining the foregoing concepts, we can create a spectrum of risk as shown in the diagram below. The following spectrum tracks real-world results. On the one hand, the algorithmic stablecoins that successfully navigated recent unprecedented price volatility and stablecoin redemptions were over-collateralized and backed by exogenous collateral (e.g. DAI, a stablecoin whose value is pegged to the U.S. dollar). On the other hand, the algorithmic stablecoins that de-pegged significantly or that failed were under-collateralized stablecoins backed almost entirely by endogenous collateral (e.g., UST). For the stablecoins that have de-pegged or failed, the primary reasons have been their collateral designs, not their algorithms.

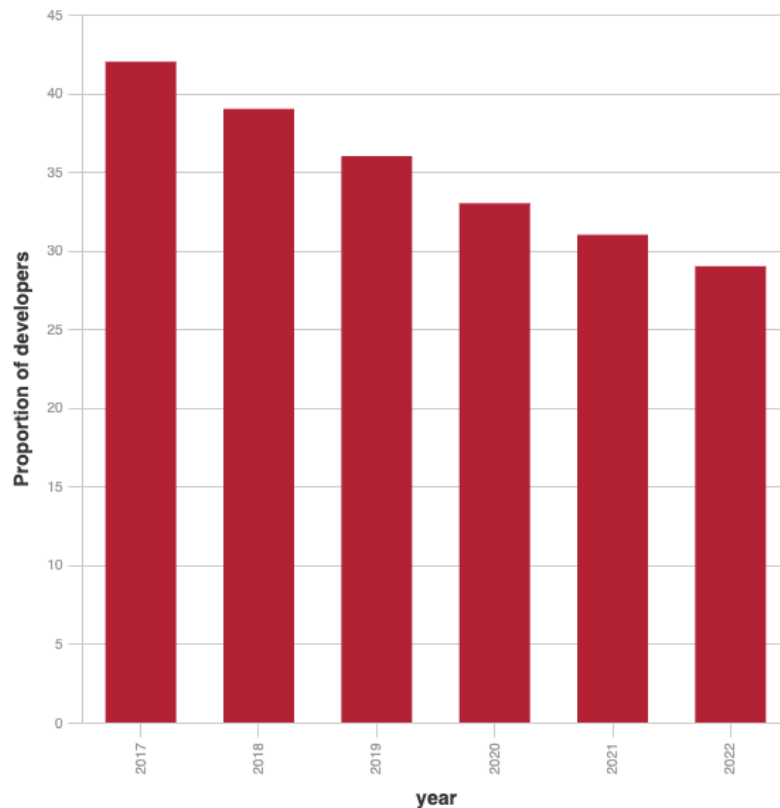


As a result of the foregoing, well-tailored stablecoin regulations should take into account the quality of the collateral being utilized to support the price of the stablecoin. Rather than banning all algorithmic stablecoins, regulations could permit the use of over-collateralized stablecoins backed solely by exogenous collateral with significant market caps (such as BTC and ETH).

II. Stablecoin regulations should be designed to keep innovation onshore.

As discussed below, the overzealous regulation of algorithmic stablecoins could be destructive to DeFi and web3, signaling to developers that the U.S. is not seeking to promote innovation and lead in web3. As a result, it is highly likely that regulatory overreach would increase the number of developers leaving the U.S. or preempt developers from coming to the U.S. to start web3 companies in the first place. This would compound an existing problem: a decline in U.S. market share with respect to web3 developers.

All crypto - Percentage of developers in the U.S.



*Electric Capital 2023*⁸

Currently, the most successful check on companies engaging in regulatory arbitrage is a combination of the following factors: (i) U.S. developers, (ii) U.S.-based investors, and/or (iii) U.S. based lawyers. The movement of developers offshore is resulting in large portions of the ecosystem no longer having any nexus (*i.e.*, connection) to the U.S. As a result, this movement has the potential to hinder the ability of the U.S. to influence the development and regulation of web3.

III. Stablecoin regulations should be designed to facilitate the propagation of U.S.-dollar-denominated stablecoins.

The market for digital property is a trillion-dollar industry and it is expected to grow. A significant percentage of the market will consist of high-quality liquid digital assets similar to BTC and ETH. If U.S. market participants cannot use those assets as collateral in algorithmic stablecoin protocols, the use of dollar-denominated stablecoins in web3 will substantially decrease. Conversely, the increase in foreign-developed web3 networks, protocols, and applications will increase the likelihood that such protocols cater to foreign-currency-denominated stablecoins from jurisdictions where fewer regulatory obstacles to web3

⁸ Herreros, E. [@eherrerosj]. (2021, March 23). Twitter. *1/ The U.S. is still losing its lead among crypto devs. We (@electriccapital) classified the location of 5000+ web3 developers using our developer data + social profiles. Let's see how fast the rest of the world is outpacing the U.S.* <https://twitter.com/eherrerosj/status/1630961162442485761?s=43&t=VW3nDYLqbZzfbpNh88vaw>.

development exist, thereby jeopardizing the role of the U.S. dollar as the reserve currency of web3 (and internet commerce) and threatening the national security of the U.S.

IV. Stablecoin regulations should limit significant financial market disruption and user losses.

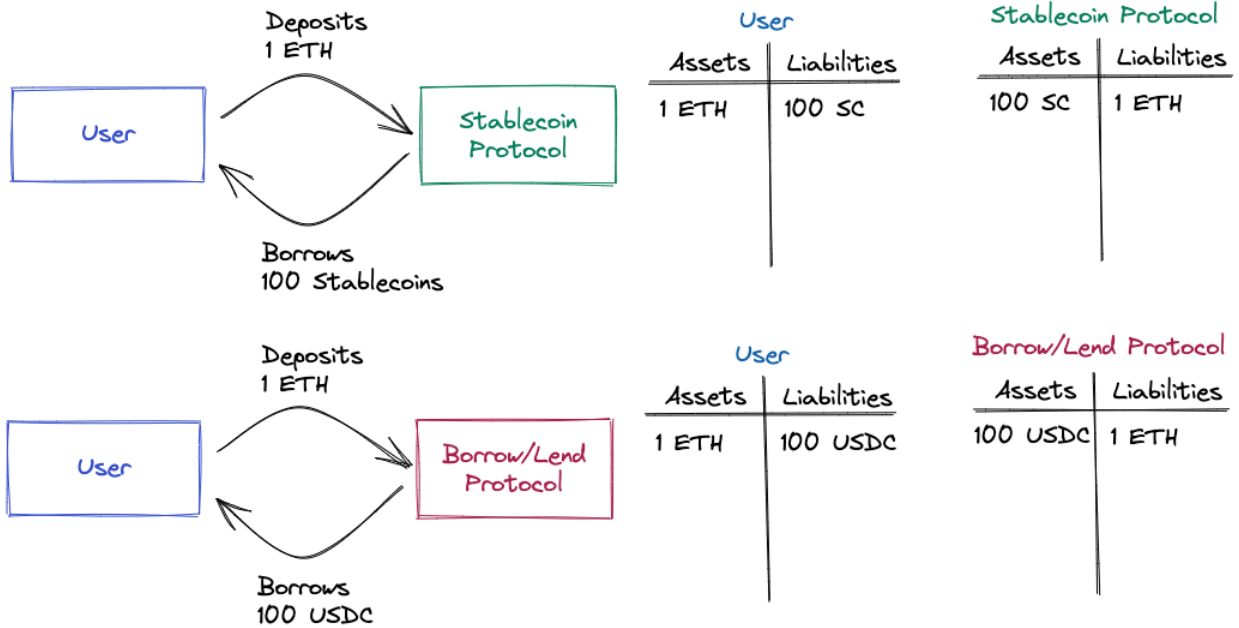
Overly restrictive regulation of algorithmic stablecoins (*e.g.*, a ban of all algorithmic stablecoins) would have drastic effects across the web3 industry. In particular, algorithmic stablecoins are integrated within thousands of DeFi protocols and are being used as collateral for borrowing and lending, as well as in trading pairs across decentralized and centralized exchanges. While these products have functioned well in orderly markets (and recent volatile markets), overly restrictive regulation like a ban could cause contagion risk that would otherwise not manifest. This would be counterproductive from both an investor protection and software development perspective, especially considering that a ban could cause even over-collateralized stablecoins to de-peg as users overreact and rush to liquidate their positions. In such a scenario, an orderly wind-down would be extremely unlikely and losses could be in the billions of dollars.⁹ The foregoing losses could compound if these protocol developers fail to participate in the liquidation and orderly winddown of such protocols. Making matters worse, these losses would be suffered by individuals who responsibly chose to hold the stablecoins that have withstood the market drawdown and that they justifiably believed to be safe.

V. Stablecoin regulations should not unnecessarily impede technological development.

Sweeping regulations targeting algorithmic stablecoins could unnecessarily undermine one of the core principles of DeFi—that automated smart contract safeguards of user funds are a suitable replacement for human intermediaries. For example, there are significant similarities between the operation of over-collateralized algorithmic stablecoin protocols, and the operation of borrowing/lending protocols (*e.g.*, Compound and Aave). These protocols allow users to deposit approved collateral (*e.g.*, ETH, BTC, etc.) with such protocols. Over-collateralized algorithmic stablecoin protocols then enable users to mint stablecoins up to the collateralization ratio approved by the Decentralized Autonomous Organization (“DAO”) of such protocol for such deposited collateral. Similarly, borrowing/lending protocols enable users to borrow other cryptocurrencies up to the DAO of the borrowing/lending protocol approved collateralization ratios for such deposited collateral.

The minting of stablecoins on the over-collateralized algorithmic stablecoin protocols entails essentially the same process of borrowing on borrowing/lending protocols; the main difference is that stablecoin protocols create the stablecoin, whereas borrowing/lending protocols lend assets they have borrowed from other users. We can see the similarities more clearly if we look at these protocols from an accounting perspective, as shown in the diagram below, because the assets and liabilities of the respective protocols are the same.

⁹ <https://coinmarketcap.com/view/stablecoin/>



In each case, the protocols utilize collateralization ratios to establish how much a user can borrow based on deposited collateral. The liquidation algorithms of these protocols then automatically execute if the value of cryptocurrency issued by the protocols (100 protocol stablecoins or 100 USDC in the diagram above) relative to the value of the collateral (1 ETH) falls below the required collateralization ratios. Such algorithms automatically liquidate the user’s collateral and sell or exchange it for the borrowed asset (the protocol’s stablecoins in the case of the stablecoin protocol, or USDC in the case of the borrowing/lending protocol).

The similar functions of these protocols extend throughout DeFi. For example, the algorithmic mechanisms they utilize are a fundamental building block of DeFi, as hundreds of other DeFi protocols use similar mechanisms. As a result, blunt and broad attacks on the algorithmic mechanisms that enable over-collateralized algorithmic stablecoin protocols to function could destabilize the DeFi ecosystem, including borrowing/lending protocols like Compound and Aave. And that destabilization would likely result in substantial losses to users—losses inflicted as a result of an attempt to protect precisely the same people that these misguided stablecoin regulations were attempting to protect.

Given the foregoing, sweeping regulation of all algorithmic stablecoins would constitute an attack on one of the critical innovations of DeFi—that users can rely on computationally enforceable commitments as a safer alternative to reliance on human intermediaries. Such an attack will likely have a significant impact on DeFi’s potential growth and future innovation within the space. That will be even more true as real-world assets migrate on-chain, and the quality of available collateral improves over time. Importantly, as e-commerce increasingly adopts web3 technology and the internet of things develops, online systems will require assets that settle instantaneously and 24/7 in a digitally native format. Future developments of algorithmic stablecoins with higher quality collateral are the most likely settlement mechanism in a web3 environment, and by shutting down algorithmic stablecoins, we would risk stifling innovation and limiting the effectiveness of these future systems.

A broad attack on algorithmic stablecoins would also have a wide array of unintended consequences across all of web3, including by limiting the ability of web3 projects and communities to make use of their own branded digital assets. This would negatively affect a variety of web3 projects, including decentralized social networks, communities enabling users to borrow and lend books, collaborative projects involving the co-creation of movies and screenplays that utilize a native digital asset to determine consensus, and video game projects with tokenized in-game assets and in-game monetary policies.

VI. Stablecoin regulations must not be impractical or counterproductive to enforce.

Several algorithmic stablecoin protocols are immutable, meaning that other than with respect to certain parameters (such as types of collateral or different collateralization ratios that they allow), they cannot be altered or removed from the blockchain where they are deployed. Further, there are hundreds of interfaces through which users can interact with such protocols, many of which themselves are decentralized or operated in international jurisdictions that do not restrict the issuance of algorithmic stablecoins.

As a result, even if they wanted to, it is implausible that legislators could completely eliminate access to algorithmic stablecoins in the U.S. and bad actors would likely copy the practices and designs of those interfaces. Such a development would likely increase regulatory arbitrage and an offshore and shadow stablecoin ecosystem would likely manifest.

Even if the U.S. government were able to eliminate all portals to stablecoin minting protocols (thereby preventing Americans from minting new algorithmic stablecoins), it would not be able to eliminate the ability of Americans to receive or use algorithmic stablecoins in their unhosted wallets without making it illegal for Americans to acquire such stablecoins. Such a restriction would be a significant intrusion on the liberty of Americans and would likely face significant legal challenges.

VII. Sensible regulatory options for algorithmic stablecoins exist.

U.S. securities laws and anti-fraud laws already provide significant protection against systemic risk from algorithmic stablecoins. As discussed above, under-collateralized stablecoins utilizing endogenous collateral present the greatest systemic risk to web3, given their potential for explosive growth and failure. They are also the most susceptible to de-peg and, as a result, are typically not as decentralized as they present themselves to be (*i.e.*, founders often retain significant control in order to drive growth and prevent failure). This level of control means that under-collateralized stablecoins utilizing endogenous collateral are often engaged in unregistered securities offerings under both *SEC v. Howey*¹⁰ as well as under *Reves v. Ernst & Young*.¹¹

Looking at UST/Terra/Luna, even prior to the network's collapse, there was significant public information available to justify the initiation of enforcement actions under Section 5 of the Securities Act of 1933, the Investment Company Act of 1940, and anti-fraud statutes. The only exogenous collateral backing UST was \$3 billion of BTC that was controlled by the Luna Foundation Guard ("LFG"), a foreign trust company that

¹⁰ 328 U.S. 293 (1946).

¹¹ 494 U.S. 56 (1990).

was, in turn, controlled by the founder of Luna. Because the success of Luna and UST were deeply intertwined, and the success of UST depended on LFG's ability to maintain UST's peg, Luna's success depended on the managerial efforts of the LFG team. As a result, per *Howey*, any issuances of Luna could have been deemed to be unregistered securities offerings.

Luna and LFG were also potentially unregistered investment companies under the Investment Company Act of 1940. Luna itself was highly centralized. It issued UST in exchange for BTC to build up LFG's BTC reserve, and it also controlled the issuance of LUNA tokens, which could be exchanged for UST.

In addition to the foregoing, enforcement action through the application of anti-fraud statutes were likely warranted. Luna had launched and controlled Anchor—a DeFi protocol built on the Terra blockchain—which increased demand for Terra. Prior to his eventual prosecution, Luna founder Kwon Do-Hyung made very public statements about the protocol and its ability to generate outsized yields from deposited Terra, which should have invited attention from enforcement authorities.¹²

An enforcement action brought under any of the foregoing theories could have substantially impeded the growth of the Luna ecosystem long before it had the potential to create systemic risk.

In addition to the fact that current regulations, if properly enforced, could prevent certain algorithmic stablecoin projects from unleashing serious harm on users and markets, blunt regulatory overreach such as a ban on algorithmic stablecoins would be unnecessary to address the risks arising due to stablecoins. More carefully tailored restrictions could all but eliminate systemic risk while minimizing the potential negative impact on the web3 industry.

For example, the U.S. could employ a tailored ban on under-collateralized algorithmic stablecoins. As discussed above, under-collateralized stablecoins that utilize endogenous collateral pose the greatest risk to users and markets. Therefore, in calculating whether or not a stablecoin is under-collateralized, all endogenous collateral would be valued at \$0. And in order to enforce this tailored ban, such under-collateralized stablecoins could be deemed securities, ensuring their prompt de-listing from centralized exchanges. Given that this proposed regulation is reasonable and measured in light of recent events, the DeFi community would likely be supportive of it and remove any such assets from DeFi applications. As a result, the utility of such stablecoins and their aggregate market caps would decrease substantially. For a real-world analog, a more measured ban in this fashion would be similar to the rules that govern margin trading, Regulation T; rather than outright banning margin loans or automatic foreclosures on margin loans, which could needlessly limit market efficiencies, the U.S. Federal Reserve sought to restrict the amount of credit brokers may extend on margin by requiring a minimum cash to margin position ratio.

Furthermore, the foregoing restrictions would be simple to enact and lead to minimal disruption in the web3 market, while protecting users against significant systemic risk in the future. Stablecoins would be well within their power to adjust their mix of collateral to comply with such a regulation and there are currently no large stablecoins that would be significantly under-collateralized under the foregoing criteria.

¹² <https://www.sec.gov/litigation/complaints/2023/comp-pr2023-32.pdf>

Conclusion

Policymakers seeking to regulate stablecoins should be focused on protecting consumers and mitigating systemic risk, but they also need to take into account a number of other considerations. This paper identifies seven such considerations:

1. **Stablecoin regulations should not treat all stablecoins as though they are the same.**
2. **Stablecoin regulations should be designed to keep innovation onshore.**
3. **Stablecoin regulations should be designed to facilitate the propagation of U.S.-dollar-denominated stablecoins.**
4. **Stablecoin regulations should limit significant financial market disruption and user losses.**
5. **Stablecoin regulations should not unnecessarily impede technological development.**
6. **Stablecoin regulations must not be impractical or counterproductive to enforce.**
7. **Sensible regulatory options exist.**

At minimum, policymakers must understand how stablecoin technology works, the promise of that technology, and the efficacy of existing regulation to meet policy objectives. In addition, they should carefully think through any proposed regulation's potential for unintended consequences—the risk of which is likely heightened in the context of stablecoin policymaking due to the increasingly borderless, open-source, and decentralized blockchain ecosystem in which stablecoins operate.

This paper maintains that algorithms are generally not the cause of stablecoin failure. Rather, stablecoin failures can usually be explained by the quality and quantity of the collateral they use, and that under- or fully-collateralized stablecoins employing endogenous collateral are at the highest risk of de-pegging. Nevertheless, additional study should be undertaken to investigate the safety of both the algorithms and collateral used amongst stablecoin protocols today.