andreessen. horowitz

December 15, 2022

BY E-MAIL

Dietrich Domanski, Secretary General
Secretariat to the Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel, Switzerland

Re: Financial Stability Board, International Regulation of Crypto-asset Activities: A Proposed Framework – Questions for Consultation; Request for Comment

Dear Mr. Domanski,

We greatly appreciate this opportunity to reply to the Request for Comment, entitled "International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation" (the "RFC"), issued by the Financial Stability Board (the "FSB") on October 11, 2022.[1] Andreessen Horowitz ("a16z") is committed to working with international officials and regulators to address the specific risks and opportunities in the blockchain and web3 ecosystems, and we commend the FSB for its commitment to soliciting information from the public through a transparent process.

We believe that blockchain technology is a momentous achievement in the development of the Internet. Since it was first developed in 2008, the blockchain ecosystem has grown rapidly, and our firm has been at the forefront of advancing the industry through investments in web3 companies that develop products and services relating to identity management, enterprise solutions, online gaming, content creation, environmental protection, data storage, and many

[1] Fin. Stability Bd., International Regulation of Crypto-asset Activities: A proposed framework – questions for consultation (Oct. 11, 2022), https://www.fsb.org/wp-content/uploads/P111022-2.pdf.

other sectors. As an industry leader, we have also assisted domestic and international regulators and officials with education around the unique attributes of decentralized systems, as well as the development of clear and robust regulatory frameworks that are appropriately calibrated to those attributes. We look forward to engaging with the FSB as well, and we hope to channel our industry observations in providing helpful feedback to the FSB's RFC.

As a preliminary matter, we believe that the FSB's principle of "same activity, same risk, same regulation" holds significant promise for the digital asset industry, but we are concerned that the principle is susceptible to two different and divergent interpretations. One interpretation, which we believe is appropriate, requires that regulators assess "activity" and "risk" as separate and independent issues before extending existing regulations to web3 businesses. The second interpretation, in contrast, involves a singular focus on the "activity," such that regulators could determine that businesses engaged in the same activities *ipso facto* pose the same risks and therefore require the same regulation. We strongly caution against the latter approach because, as discussed below, certain web3 businesses solve some legacy risks while presenting newer, unique risks when compared to traditional finance, even when their services resemble one another. In addition, we encourage the FSB to consider whether a more effective method for meeting its intended goals would be to seek the "same outcome," rather than the "same regulation."

In this comment letter, we focus on three areas of "activity" and "risk" identified in the RFC — decentralized finance ("DeFi"), mitigating illicit finance, and algorithmic stablecoins — that resemble traditional finance in services offered, but involve risks unique to their structures. Given the unique risks of these products and services, we believe that the FSB should recommend a new, tailored regulatory framework to oversee them, rather than extending existing regulations under a "one-size-fits-all" approach. This comment letter is divided into three parts:

First, we discuss the differences between centralized finance ("CeFi") and DeFi, and how an appropriately tailored regulatory framework for DeFi should involve regulating web3

applications, not web3 protocols ("regulate businesses, not software"). ***Second***, we discuss the importance of privacy, while still mitigating illicit finance risk. ***Lastly***, we caution against overly restrictive regulations that could have the effect of banning well-functioning and over-collateralized algorithmic stablecoins, and we suggest that collateralization requirements could mitigate risks.

I. About a16z

Andreessen Horowitz, also referred to as a16z, is a venture capital firm that backs entrepreneurs building the future through technology. We invest in seed, venture, and late-stage technology companies, focused on bio/healthcare, consumer, crypto, enterprise, fintech, and games. The firm currently has $35 billion in committed capital under management across multiple funds.

a16z aims to connect entrepreneurs, investors, executives, engineers, academics, industry experts, and others in the technology ecosystem. We have built a network of experts, including technical and executive talent, top media and marketing resources, Fortune 500/Global 2000 companies, as well as other technology decision makers, influencers, and key opinion leaders. a16z uses this network as part of our commitment to helping our portfolio companies grow their businesses.

At a16z, we believe we need an Internet that can foster competition and mitigate the dominance of large technology companies, unlock opportunities for the millions on the margins of the innovation economy, and enable people to take control of their digital information. The solution is web3 — the third generation of the Internet — a group of technologies that encompasses digital assets, decentralized applications and finance, blockchains, tokens, and decentralized autonomous organizations. Together, these tools enable new forms of human collaboration. They can break through the stalemates that define too many aspects of public life and help communities make better collective decisions about critical issues, such as how

networks will evolve and how economic benefits will be distributed. We are radically optimistic about the potential of web3 to restore trust in institutions and expand access to opportunity.

II. Decentralized Finance

DeFi applications are among the most important emerging technologies in the blockchain ecosystem that do not lend themselves to existing financial regulatory frameworks. That is because DeFi applications were built as an alternative to trusted financial intermediaries — the primary targets of traditional regulatory frameworks.[2] Traditional frameworks do not take into consideration the radical transparency of blockchains, the reduced barriers to entry provided by open source code, and the advantages of decentralization provided by permissionless systems.[3] This design of DeFi is "trustless" because it allows users to engage in peer-to-peer transactions without reliance on third parties, it eliminates significant risks relating to information asymmetries that characterize traditional markets, and it allows users to maintain more control over their assets relative to traditional finance. The approach of investors to traditional financial intermediaries, in contrast, is "trust but verify." Because intermediaries typically have no incentive to meet the informational needs of investors and have none of the transparency characteristics of DeFi, the existing financial regulatory frameworks must mandate disclosures in order to increase trust in the financial system.

That said, DeFi can pose unique risks that existing regulatory frameworks are ill-suited to cover. For that reason, a new regulatory framework is optimal, and as explained below, we believe that the framework should be based on the principle of regulating DeFi applications and businesses, not protocols. Businesses can comprehend and comply with jurisdictional regulations. Globally accessible software cannot.

---

[2] John Coffee, Hillary Sale & M. Todd Henderson, Securities Regulation: Cases and Materials, at 3 (13th ed.) (Foundation Press, 2015).

[3] *See Cryptocurrency Terms to Know*, WorldCoin, https://worldcoin.org/articles/cryptocurrency-terms-to-know (last updated Nov. 29, 2022) (stating that "[d]ecentralized blockchains are permissionless, which means users don't require permission to participate. Everyone can gain access to and participate in a cryptocurrency's blockchain.").

A. CeFi Versus DeFi: How the Markets Differ

Many people confuse "crypto CeFi" with DeFi because both are a means for customers and users to participate in crypto markets.[4] But CeFi and DeFi operate in fundamentally different ways, and it is precisely because of their unique characteristics that we support distinct regulatory frameworks for each.

As an initial matter, CeFi institutions, as the name implies, are "centralized" operations, complete with management teams and conflicts of interest, where users interact with third-party intermediaries to access crypto markets.[5] The intermediaries are typically traditional private businesses, where users are customers of the business, and decisions about how to run the business are made behind closed doors. On the other hand, DeFi is made up of software protocols that provide a number of disintermediated financial products and services. These software protocols typically consist of a collection of smart contracts deployed to a decentralized blockchain. Users can interact with these protocols directly, without intermediaries, to trade financial products in peer-to-peer transactions,[6] and the rules that govern DeFi protocols are written in and enforced through computer code. This has particular importance in jurisdictions where financial regulation is inappropriately weak, or where trust in institutions, whether political, financial, or both, is compromised. There are also benefits to contagion risk, as transparent transactions and on-chain exposures reduce the possibilities for opaque leveraged positions and enhance risk management through a more transparent level of interconnectedness.

---

[4] CeFi and DeFi are not to be confused with traditional financial markets ("TradFi"), where users seek to participate in non-crypto markets. *See* Dushyant Shahrawat, *Claims That DeFi Is Unraveling Or Structurally Flawed Are Unfounded*, Forbes (July 27, 2022), https://www.forbes.com/sites/dushyantshahrawat/2022/07/27/claims-that-defi-is-unraveling-or-structurally-flawed-are-unfounded/?sh=782346af491d.

[5] *What Is CeFi (Centralized Finance)?*, WorldCoin, https://worldcoin.org/articles/what-is-cefi (last updated Dec. 1, 2022); *see also* Ekin Genç, *DeFi vs. CeFi in Crypto*, CoinDesk (Aug. 15, 2022), https://www.coindesk.com/learn/defi-vs-cefi-in-crypto/.

[6] *Decentralized finance (DeFi)*, Ethereum, https://ethereum.org/en/defi/ (last updated Dec. 14, 2022).

Because DeFi relies on code instead of intermediaries, DeFi protocols are extremely transparent. Generally, anyone can inspect and audit the public blockchain ledgers upon which many DeFi protocols are built, and the ledgers reflect both the smart contracts that govern the protocol's operations, as well as a record of the price and quantity of each transaction entered into on a given platform.[7] For example, Compound,[8] a popular DeFi lending protocol, has a transparent, immutable, and publicly inspectable ledger of all historical transactions.[9] Importantly, this information is available in near real-time. In contrast, CeFi intermediaries are opaque, such that the public receives required information on a limited, sporadic, and after-the-fact basis. Given the transparency of DeFi systems utilizing open source code and on-chain tracking, it is comparatively easy for regulators and users to monitor them in ways that are not available with respect to CeFi intermediaries.

To date, DeFi protocols have demonstrated significant resilience to market pressures, especially when compared to CeFi intermediaries. In recent months of market volatility, large scale bankruptcies in the crypto markets have been concentrated among CeFi institutions,[10] like Celsius Network and Voyager Digital, while truly decentralized DeFi protocols, like the

[7] Sarit Markovich et al., *Transparency and Learning: Evidence from Defi Markets*, at 1 (Nov. 12, 2021), https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3962517_code80819.pdf?abstractid=3962517&mirid=1.
[8] a16z Crypto is an investor in Compound. *See* Leigh Cuen, *DeFi Startup Compound Finance Raises $25 Million Series A Led by A16z*, CoinDesk (Nov. 14, 2019), https://www.coindesk.com/tech/2019/11/14/defi-startup-compound-finance-raises-25-million-series-a-led-by-a16z/ (last updated Sept. 13, 2021). A list of investments made by a16z managed funds is available at https://a16z.com/investments/.
[9] *See* Robert Leshner & Geoffrey Hayes, *Compound: The Money Market Protocol*, Compound (Feb. 2019), https://compound.finance/documents/Compound.Whitepaper.pdf.
[10] Catarina Moura, *Crypto bankruptcy filings: From 3AC to BlockFi*, The Block (Nov. 28, 2022), https://www.theblock.co/post/190354/crypto-bankruptcy-filings-from-3ac-to-blockfi.

Compound[11] lending protocol and the Uniswap exchange,[12] have continued operating without interruption or compromise.[13] That comparative success is both a function of DeFi protocols' smart contract integrity, and transparency. Given those strengths, we believe that the DeFi ecosystem will continue to grow in use, utility, and complexity over the coming years.

B. A New Regulatory Framework for DeFi: Regulating Applications, Not Protocols

As mentioned above, we believe that an appropriately tailored regulatory framework for DeFi involves the regulation of the centralized/business-owned applications, or onboarding access points to protocols, not the protocols or software themselves. As discussed below, this distinction — between business-owned applications and protocols — is crucial.

---

[11] Compound is a decentralized lending protocol that operates on the Ethereum blockchain and establishes money markets. The protocol works by allowing users to deposit cryptocurrencies as collateral, and in return, Compound provides depositors with a token, known as the "cToken" that matches the deposited collateral, e.g., "cETH" or "cDAI" in the case of deposited ETH or DAI, respectively. The protocol will mint a "cToken" for any supported tokens, and all cTokens are redeemable for the cryptocurrencies that were initially locked in the protocol and any associated interest paid. Each loan on the protocol is over-collateralized to protect against price fluctuations among the cryptocurrencies that serve as collateral. Another token within the Compound network is its governance token, known as "COMP." *See* Leshner & Hayes, *supra* note 9.

[12] a16z Crypto is an investor in Uniswap. *See* Hayden Adams, *Bringing Web3 to Everyone*, Uniswap Blog (Oct. 13, 2022), https://uniswap.org/blog/bringing-web3-to-everyone.
The Uniswap protocol is a decentralized exchange that operates on the Ethereum blockchain and facilitates automated transactions between cryptocurrency tokens through the use of smart contracts. *See* Uniswap Protocol, https://uniswap.org/. Critical to the Uniswap system is its use of an automated marketmaker. More specifically, unlike centralized exchanges that use a traditional order book system to facilitate trading — where a buy order is matched with a sell order for the same amount and price of an asset — Uniswap uses an automated liquidity protocol. This protocol functions by allowing users to pool their tokens together in "liquidity pools" to create funds that are used to execute trades on the platform. Users that want to sell or purchase a certain token can "swap" their tokens with tokens in the liquidity pools. There is a liquidity pool for each token listed on the protocol, and an algorithm run by a computer calculates the price of each token. *See* Ollie Leech, *What Is Uniswap? A Complete Beginner's Guide*, CoinDesk (Nov. 16, 2022), https://www.coindesk.com/business/2021/02/04/what-is-uniswap-a-complete-beginners-guide/.

[13] Shai Bernstein & Scott Duke Kominers, *Why Decentralized Crypto Platforms Are Weathering the Crash*, Harv. Bus. Rev. (Dec. 7, 2022), https://hbr.org/2022/12/why-decentralized-crypto-platforms-are-weathering-the-crash?ab=hero-main-text.

a. DeFi Protocols

DeFi protocols are software programs consisting of smart contracts that provide the functionality for peer-to-peer lending, borrowing, and other financial transactions. Protocols are hosted on or integrated in blockchains, such as Ethereum,[14] and they are open-source, decentralized, autonomous, and censorship resistant. Of these characteristics, decentralization and censorship resistance have particular regulatory and political significance.

- Decentralization is a broad term that refers to multiple aspects of a blockchain, including political/legal decentralization (because no one controls public blockchains) and architectural decentralization (because there is no central point of failure).[15] As many regulators have noted, decentralization is a spectrum, with some web3 businesses starting off centralized and transitioning toward a decentralized model. We have suggested that a "sufficiently" decentralized web3 entity exists where (i) information regarding its operation is transparent and available to all (enabled by transparent blockchain ledgers) and (ii) no essential managerial efforts are necessary (or even possible) to drive the success or failure of the enterprise (enabled by immutable smart contracts, decentralized economies, and DAOs). We have linked our more extensive findings on this issue below.[16]

- Censorship resistance, like decentralization, is also a broad term that describes the ability of almost anyone to use public blockchains, as well as the fact that no one can be kicked

[14] Lindsay X. Lin, *Deconstructing Decentralized Exchanges*, Stan. J. Blockchain L. & Pol'y (2015), https://stanford-jblp.pubpub.org/pub/deconstructing-dex; *see also* Fred Ehrsam, *Why Decentralized Exchange Protocols Matter*, Medium (Sept. 27, 2017), https://medium.com/@FEhrsam/why-decentralized-exchange-protocols-matter-58fb5e08b320.
[15] Vitalik Buterin, *The Meaning of Decentralization*, Medium (Feb. 6, 2017), https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
[16] Miles Jennings, *Principles & Models of Web3 Decentralization*, Andreessen Horowitz (Apr. 2022), https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralization_miles-jennings_a16zcrypto.pdf.

off of a public blockchain.[17] It also describes the fact that no one on the blockchain is independently powerful enough to block transactions or prevent others who wish to validate blockchain transactions from joining the consensus network.

Because no one controls the protocol, a protocol cannot incorporate subjective determinations that traditional finance regulations sometimes require, and therefore, they cannot comply with, or comprehend, specific jurisdictional requirements. For instance, product classifications, such as securities, commodities, and various derivatives instruments, differ between jurisdictions and can be highly subjective from country to country. Globally accessible software can neither apply facts and circumstances tests, nor incorporate inconsistencies in its programing. Further, regardless of changes in law or regulations, DeFi protocols, like the Uniswap protocol, once deployed, will function in perpetuity as originally constructed, since their design parameters generally severely limit functionality updates.[18] In the event that a web3 community votes for a proposal to update to a new version of a DeFi protocol or launch a new version of the protocol, applications providing users with access to the earlier version update their codebases to point to the new version's smart contracts.

b. DeFi Applications

DeFi applications are products built on top of DeFi protocols that allow users to access the protocols. Importantly, they typically add an on-chain or off-chain order book database, and a graphic user interface (GUI) or APIs or both.[19] Unlike the protocol layer, businesses and developers of web3 applications do not have the same constraints with respect to subjective determinations. They can comply with different jurisdictional regulations and design flexible

[17] Vitalik Buterin, *The Problem of Censorship*, Ethereum Foundation Blog (June 6, 2015), https://blog.ethereum.org/2015/06/06/the-problem-of-censorship; *see also* Gregory Rocco, *Public Blockchains as a Means to Resist Information Censorship*, CUNY Academic Works (Feb. 2019), https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=4048&context=gc_etds.
[18] *See The Uniswap Protocol*, https://docs.uniswap.org/concepts/uniswap-protocol.
[19] *See* Lin, *supra* note 14.

access points that minimize legal and regulatory risks. We have written extensively about the "regulate apps, not protocols" principle, and our findings are linked below.[20]

c. Traditional CeFi Regulations Should Not be Applied to DeFi

Regulations designed for CeFi should not be applied to DeFi wholesale as they are not well tailored to the differences between the two types of products and services. In the world of CeFi, many regulations are designed to remove the risk of trusting financial intermediaries. The goal is to reduce the risks that may arise whenever there is a potential for conflicts of interest or outright fraud, which may occur when one person has to trust another with their money or assets.[21] In the world of DeFi, where traditional financial services are disintermediated, there are no intermediaries to trust. Accordingly, in DeFi, the decentralization, transparency, and trustlessness enabled by blockchain technology eliminates much of the risk that many CeFi regulations are primarily intended to address. DeFi can therefore insulate users from many of the age-old acts of malfeasance prevalent in CeFi and do so better than any "self-regulatory" or "public regulatory" regime in CeFi ever could.

As a result, the wholesale application of CeFi regulations to decentralized web3 apps that do not provide intermediary-like services is illogical. Moreover, any regulatory intervention would be counterproductive, as it would impede DeFi's native ability to effectuate the very legitimate policy objectives that many financial regulations pursue, such as transparency, auditability, traceability, responsible risk management, and so forth. Imagine the value destruction of forcing the SMTP email protocol to abide by various jurisdictions' regimes, from free speech legal enforcement to data privacy laws like GDPR. However, applications accessing SMTP to talk to each other can comply — Gmail for instance, could comply with various regulatory requirements or be responsive to regulatory information requests. Traditional regulation at the protocol level is unworkable.

---

[20] *See* Miles Jennings, *Regulate Web3 Apps, Not Protocols*, Andreessen Horowitz (Sept. 29, 2022), https://a16zcrypto.com/web3-regulation-apps-not-protocols/.

[21] *See* FTX, Celsius Network, Voyager Digital, 3AC, MF Global, Revco, Fannie Mae, Lehman Brothers, AIG, Long-Term Capital Management, and Bernie Madoff.

d. An Appropriately Tailored Regulatory Framework is Critical for Guaranteeing DeFi's Benefits

We also believe that the principle of regulating applications, and not protocols, is critical for guaranteeing the transparency and trustlessness benefits of DeFi for the international financial system. As described above, because DeFi applications operate on blockchain technology, they are open and accessible to anyone around the world, which creates unprecedented opportunities for access to financial services. Since January 2020, DeFi adoption has ballooned, increasing from about 91,000 to almost 5 million users,[22] with its benefits accruing most clearly in those emerging markets where trust in political authorities and financial institutions may be compromised. Latin American countries lead the world in DeFi adoption, particularly in areas where credit facilities are scarce.[23] DeFi is also making inroads in African countries, like Nigeria and Kenya.[24]

The adoption of a regulatory framework that captures the software infrastructure that fuels the web3 ecosystem, rather than the applications which operate as access points, could jeopardize the benefits of DeFi for millions of people, and push protocol developers to jurisdictions with particularly loose regulatory frameworks.[25] If regulators were to impose subjective and potentially globally conflicting regulations — such as what may or may not be a

---

[22] *See* Anna Stone, *Why decentralized finance is a leapfrog technology for the 1.1 billion people who are unbanked*, World Economic Forum (Sept. 16, 2022), https://www.weforum.org/agenda/2022/09/decentralized-finance-a-leapfrog-technology-for-the-unbanked/.

[23] Chainalysis Team, *Latin America's Key Crypto Adoption Drivers: Storing Value, Sending Remittances, and Seeking Alpha*, Chainalysis (Oct. 20, 2022), https://blog.chainalysis.com/reports/latin-america-cryptocurrency-geography-report-2022-preview/.

[24] Bitange Ndemo, *The Role of Cryptocurrencies in sub-Saharan Africa*, Brookings Institute (Mar. 16, 2022), https://www.brookings.edu/blog/africa-in-focus/2022/03/16/the-role-of-cryptocurrencies-in-sub-saharan-africa/.

[25] FinCEN has correctly recognized that suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001, at 20, 23–24 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

security, commodity, or derivative of each — on web3 protocols, decentralization would be untenable, undermining the very properties that make DeFi protocols functional and useful in the first place. We believe international officials and regulators can most effectively meet this challenge by promoting responsible development of the DeFi industry, especially through the creation of a clear and workable legal framework based on regulating DeFi applications.

III. Privacy and Mitigating Illicit Finance and National Security Risk

Having a clear and consistent global regulatory framework to strengthen financial integrity and combat money laundering and terrorist financing is critical to the maturation of the digital asset sector. We know that such a framework would be most successful if supported by proactive collaboration and real-time information sharing between the public and private sectors to mitigate the risk of money laundering, terrorist financing, and other illicit activity.

We applaud the consultative approach of the Financial Action Task Force ("FATF") in developing recommendations and guidance on anti-money laundering ("AML") and combating the financing of terrorism ("CFT") in the digital asset sector.[26] As the sector continues to innovate, the FATF should continue to consult with the private sector, and its members should engage in hands-on experimentation with the technology in order to develop policies that most effectively accomplish necessary goals while avoiding overbroad or unintended consequences. Moreover, local regulators should similarly engage the digital asset industry as they implement FATF's virtual asset standards.

In the United States, many cryptocurrency businesses are covered by the U.S. Bank Secrecy Act, and those covered entities have successfully drawn from the AML programs of traditional financial institutions while also developing additional elements reflective of the unique circumstances of crypto. Additionally, the U.S. Financial Crimes Enforcement Network

[26] Fin. Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations*, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf (last updated Mar. 2022).

("FinCEN") has worked closely with crypto-asset service providers to leverage its advanced information and threat-detection capabilities. But, Know-Your-Customer ("KYC") rules, where applicable, should be fit-for-purpose, using the technical capabilities of blockchain technology. KYC processes that collect the minimum amount of identifiable user data should be encouraged, as should experimentation with technologies and processes via exceptive relief and regulatory sandboxes. This flexible approach can facilitate the development of crypto-native tools that leverage blockchain technology and transparency to effectively combat illicit finance.

Notwithstanding these important compliance obligations for covered entities, privacy is a fundamental human right and social good. Privacy-preserving technology allows data computation and targeted analysis while remaining encrypted to those performing the computation and to malicious actors who might seek to steal or corrupt that information. Zero-knowledge proofs and configurable privacy blockchains are emerging forms of privacy-preserving technologies that have the ability to balance individuals' privacy interests with broader public policy and societal requirements, such as effective compliance, transparency, and safety.

Governments should adopt laws and policies that allow for the development and use of privacy-preserving technologies, while also enabling compliance. For example, regulators could establish processes to evaluate the way novel mechanisms can be used to create and maintain digital identity records, including the adoption of digital identity verification techniques that can use a combination of decentralized blockchain-based technologies and secure "off-chain" data repositories. Moreover, zero-knowledge proof technology could be used to conduct sanctions screening. For a more thorough discussion of this topic, see our white paper linked below.[27] Regulators could also encourage use of these technologies by intermediaries as a more effective way of countering broader illicit finance risks in addition to sanctions compliance.

[27] Joseph Burleson et. al, *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs*, Andreessen Horowitz (Nov. 16, 2022), https://a16zcrypto.com/wp-content/uploads/2022/11/ZKPs-and-Regulatory-Compliant-Privacy.pdf.

Concurrently, governments should respect personal privacy themselves by accessing or using data on individuals only when doing so is necessary to further a specific, narrowly tailored, and legitimate governmental objective. For example, the U.S. Department of the Treasury's proposal under consideration to collect, verify, and retain the names and physical addresses of all counterparties to transactions over $3,000 between cryptocurrency exchanges and unhosted wallets poses serious privacy and security concerns. Moreover, such proposals could harm law enforcement investigations, prosecutions, and asset recovery capabilities by driving self-hosted wallet users from well-regulated and compliant exchanges and financial intermediaries to non-compliant or poorly supervised entities, decreasing the amount of valuable information available to law enforcement and national security agencies.

Finally, we recommend that the FSB clarify that its statement in high-level recommendation 5 of the GSC report that "authorities should ensure that GSC arrangements put appropriate AML/CFT measures in place consistent with FATF Standards, including requirements to comply with the FATF 'travel rule', with specific consideration if the GSC arrangements allow peer-to-peer transactions by unhosted wallets,"[28] applies only to those covered entities with travel rule obligations, and not generally to unhosted, or non-custodial, wallet providers, users, or non-VASP entities.

IV. Algorithmic Stablecoins

The FSB's recommendation for stablecoins — that reserve assets should be "at least equal" to the amount of an issuer's outstanding stablecoins[29] and consist only of "conservative" assets, and that stablecoins should not "derive" their value from algorithms — would result in negative unintended consequences for the blockchain ecosystem.[30] More specifically, we are

[28] Fin. Stability Bd., Review of the FSB High-level Recommendations of the Regulation, Supervision and Oversight of "Global Stablecoin" Arrangements, Consultative Report, at 16 (Oct. 11, 2022), https://www.fsb.org/wp-content/uploads/P111022-4.pdf [hereinafter: "FSB Global Stablecoin Consultative Report"].
[29] While we understand that the FSB recommendation excepts entities subject to prudential regulations, the majority of stablecoin issuers do not fall within that category.
[30] *See* FSB Global Stablecoin Consultative Report, at 20.

concerned that a framework based on this recommendation would effectively ban algorithmic stablecoins — the best of which operate through over-collateralization by exogenous collateral — and signal hostility toward web3 applications that rely on algorithms to develop products and services. While we wholeheartedly support regulation that prevents stablecoin issuers from taking on unreasonable amounts of risk, we believe that lawmakers can protect users without such broad bans. And they can do this by enacting narrowly tailored collateralization requirements that allow for the development of safe software code but prevent overly risky projects.

A. Algorithms Are Not The Problem

Stablecoins are cryptocurrencies whose value is tied, or pegged, to the value of an outside asset, like the U.S. dollar or gold. A stablecoin can maintain the peg by custodying the collateral and reserve assets through centralization, or by using a combination of algorithmic clearing mechanisms and collateral consisting of different cryptocurrencies or other assets. As a general matter, lawmakers and regulators commonly focus on stablecoins that employ algorithms, i.e., algorithmic stablecoins, as a risk area.

But that overly broad concern is largely misplaced because it focuses on algorithms as a source of instability, rather than the real problem — under-collateralization. Nearly one year into the current market volatility, we now know that the vast majority of algorithmic stablecoin projects have performed remarkably well, and the exceptional few that did not were significantly under-collateralized and they relied on collateral created by the issuers themselves.[31] Importantly, the reason for the relative safety of algorithmic stablecoins was precisely because of the blockchain programmability that creates certain key risk controls typical in traditional clearing infrastructure, including, among other things, the liquidation of collateral, which protected investors and the protocols' safety and soundness far more transparently and efficiently than a manual process would have.

[31] *See* Miles Jennings, *In defence of stablecoins*, Financial Times (Aug. 7, 2022), https://www.ft.com/content/39681aa2-aa01-4d60-b399-8ecb236c627e.

One example of blockchain programmability involves stablecoins that require users to deposit ETH as collateral. These protocols require that the value of the ETH collateral be worth between 135% and 150% (the "Collateralization Ratios") of the value the users intend to mint in the stablecoins of such protocols. While those stablecoins are outstanding, if the price of ETH declines such that the value of users' collateral is below the Collateralization Ratios for the protocols, the users' collateral is automatically liquidated, and their ETH is sold to close out the loaned stablecoin the users minted. All of this happens automatically and autonomously, ensuring that the collateral of the protocols never falls below the value of the outstanding stablecoin.[32]

Given the success of over-collateralized stablecoins over heavily volatile periods, such programmable safety mechanisms should be commended, not discouraged.

B. Regulating Algorithmic Stablecoins

The FSB has a great opportunity to recommend an appropriately tailored regulatory framework for algorithmic stablecoins that recognizes the important role of algorithms and digital assets. But the recommendation, as currently drafted, all but explicitly calls for an effective ban on algorithmic stablecoins, as it generally requires 1:1 backing of all stablecoins in conservative and highly liquid assets, suggests limiting the use of crypto as reserves, and states that a stablecoin should not "derive its value from algorithms."[33]

More carefully tailored requirements will be more effective in protecting both the blockchain ecosystem and users. The FSB should conduct a study analyzing the relative safety of over-collateralized stablecoins to assess which collateral and Collateralization Ratios might be sufficient to permit the continued use of such collateral. For example, a regulatory proposal could feasibly recommend that only digital assets with a market capitalization in excess of a

[32] For a more specific example of blockchain programmability, *see* Leshner & Hayes, *supra* note 9, at 4 ("Risk & Liquidation").
[33] *See* FSB Global Stablecoin Consultative Report, at 20.

certain dollar threshold be used as collateral to ensure that bad actors cannot easily manipulate the collateralized assets. Further, Collateralization Ratios above 125% have proven themselves to be effective in the recent volatility and are worth further exploring.

A broad ban of algorithmic stablecoins, on the other hand, could harm the international financial system. For one, stablecoins, both custodial and algorithmic, provide stability in countries where centralized monetary policy has failed.[34] And as more countries face growing inflation pressures, we expect stablecoin usage to increase.[35] Moreover, algorithms are not only important to stablecoin development, they are also key to other aspects of the blockchain ecosystem, including DeFi and other digital asset markets. If regulators focus on algorithms as a source of instability, web3 developers may perceive a threat toward their projects and exit the market. With appropriately tailored regulations, we can prevent this outcome.

In short, our high-level principles with respect to algorithmic stablecoins are:

- **A ban will unnecessarily treat all algorithmic stablecoins alike, when they are actually very different.** The systemic risk posed by stablecoins is more a product of the design of their collateralization than their use of algorithms. A ban on all algorithmic stablecoins is like using a sledgehammer to crack a nut.

- **A ban will disrupt the current DeFi market and result in significant customer losses.** A ban would be damaging and counterproductive from both an investor protection and software development perspective, potentially resulting in billions of dollars of losses for precisely the same users that policymakers are trying to protect.

---

[34] *See* Chainalysis Team, *supra* note 23; *see also* Sebastian Serrano, *Saving (in) Latin America: Why stablecoins are thriving across emerging markets*, Circle (Oct. 14, 2020), https://www.circle.com/blog/saving-in-latin-america-why-stablecoins-are-thriving-across-emerging-markets.

[35] Thirty countries are experiencing rates of inflation at approximately 20% or more. The top five worst countries for inflation are Sudan (103%), Syria (139%), Venezuela (156%), Lebanon (158%), and Zimbabwe (255%). *See Inflation Rate* / *World*, Trading Economics, https://tradingeconomics.com/country-list/inflation-rate?continent=world (last visited Dec. 15, 2022).

- **A ban will have unforeseen and negative consequences throughout DeFi and the broader web3 industry.** The algorithmic mechanisms utilized by algorithmic stablecoin protocols are prevalent across DeFi and web3. The blockchain ecosystem could view a blanket ban on algorithmic stablecoins as an attack on these mechanisms, which could inadvertently hinder a wide array of web3 innovation.

- **A ban will be extremely difficult to enforce.** Various global jurisdictions choosing to implement an FSB-sanctioned ban will be unable to remove all algorithmic stablecoins from their markets, and a ban is therefore likely to encourage regulatory arbitrage, putting users at greater risk of harm.

- **A ban will push innovation to regions with particularly loose regulatory frameworks and hurt large, well-regulated, and developed economies.** A ban could accelerate the developed world's declining market share of web3 developers and hinder its ability to influence the web3 and broader industry's development.

- **A ban is unnecessary as alternative restrictions would be more effective at reducing systemic risk.** Regulators could have utilized existing regulations to prevent much of the recent systemic harm, and new precise regulation could eliminate the risk of such systemic harm being repeated without hindering innovation.

V. Conclusion

It is critically important that regulators and policy leaders thoughtfully regulate blockchain technology, as it is rapidly becoming a key pillar of the financial system, and we greatly appreciate the opportunity to provide comments on these important matters. We view this comment letter as part of an ongoing dialogue between the public and private sectors and look forward to continued engagement on these issues.

Respectfully submitted,

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Miles Jennings, General Counsel and Head of Decentralization
a16z Crypto

Michele R. Korver, Head of Regulatory
a16z Crypto

Brian Quintenz, Head of Policy
a16z Crypto