November 3, 2022

BY E-MAIL AND ELECTRONIC SUBMISSION

Scott Rembrandt, Deputy Assistant Secretary
Office of Terrorist Financing and Financial Crimes
U.S. Department of the Treasury
Three Lafayette Center
1500 Pennsylvania Avenue, NW
Washington, D.C. 20220

Re: Ensuring Responsible Development of Digital Assets; Request for Comment

Dear Mr. Rembrandt,

We greatly appreciate this opportunity to comment on the Request for Comment, entitled "Ensuring Responsible Development of Digital Assets" (the "Request"), issued by the Department of the Treasury ("Treasury") on September 20, 2022, seeking information on digital-asset-related illicit finance and national security risks.[1] Andreessen Horowitz ("a16z") is committed to working with both federal and state officials to address risks in the blockchain and web3 ecosystems, and we commend Treasury for its commitment to soliciting information from the public through a transparent process.

Blockchain technology is a momentous achievement in the development of the Internet. Households previously locked out of the financial markets now have access to credit and other

[1] U.S. Dep't of the Treasury, Ensuring Responsible Development of Digital Assets; Request for Comment, TREAS-DO-2022-0018-0001, 87 FR 57556 (Sept. 20, 2022), https://www.govinfo.gov/content/pkg/FR-2022-09-20/pdf/2022-20279.pdf.

financial opportunities through decentralized finance ("DeFi").[2] Artists and other content creators can monetize their work using non-fungible tokens ("NFTs") without the need for commercial middlemen.[3] And other market participants use blockchain technology in industries that range from identity management, enterprise solutions, online gaming, and data storage. The American economy has already reaped tremendous rewards from the proliferation of high quality American jobs in the blockchain industry.[4]

But that said, we also recognize that the promise of blockchain technology, like any new technology, has potential risks. And we appreciate that the blockchain and web3 ecosystems cannot thrive without sufficient safeguards to mitigate against them. It is for these reasons that we previously led fundraising rounds for web3 companies like Forta, an enterprise-grade runtime security platform whose goal is to detect threats and other system critical issues as quickly as possible,[5] and Spruce Systems, a decentralized identity startup.[6] We have also invested in privacy protocols, which strengthen national security by making it more difficult for adversaries of the United States, such as China and Russia, to steal and exploit the personal data of American citizens and businesses.

We hope to channel our industry observations in providing helpful feedback to Treasury's Request, and we believe that our expertise is most relevant to the questions in Section III.A. relating to illicit finance risks.

---

[2] *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/.

[3] *See* Chris Dixon, *NFTs and a Thousand True Fans*, Future (Feb. 27, 2021), https://future.com/nfts-thousand-true-fans/; *see also* Daren Matsuoka et al., *Introducing the 2022 State of Crypto Report*, Andreessen Horowitz (May 17, 2022), https://a16zcrypto.com/state-of-crypto-report-a16z-2022/.

[4] Post of LinkedIn News (Jan. 2022), https://www.linkedin.com/posts/linkedin-news_theworkshift-economy-labormarket-activity-6887062336839016450-67iT/.

[5] Arianna Simpson, *Investing in Forta*, Andreessen Horowitz (Sept. 30, 2021), https://a16z.com/2021/09/30/investing-in-forta/.

[6] Eddy Lazzarin & Chris Dixon, *Investing in Spruce*, Andreessen Horowitz (Apr. 21, 2022), https://a16z.com/2022/04/21/investing-in-spruce/.

This comment letter is divided into five parts: ***First***, we discuss the benefits of privacy-preserving technologies and enhancements, and how they can be designed and used to mitigate illicit finance risks. ***Second***, we describe the embedded transparency of the DeFi markets and explain how an appropriately tailored regulatory framework would involve regulating web3 applications, not web3 protocols. ***Third***, we recommend the use of existing authorities to address illicit finance facilitators. ***Fourth***, we describe the unique characteristics of NFTs and how those characteristics can mitigate illicit finance risks. ***Lastly***, we identify web3 entities that are working to enhance blockchain cybersecurity and recommend that the government support such efforts.

This comment letter also serves as a supplement to the comment letter from the Crypto Council for Innovation ("CCI"), a trade association of which we are a member. We wholeheartedly support CCI's response, which focuses on different topics in the Request, in particular the importance of public-private information sharing and collaboration.

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 help the United States retain leadership in a world of increasing competition, unlock opportunity 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. Mitigating Illicit Finance Risks

Since blockchain technology was first developed in 2008, the web3 ecosystem has successfully integrated effective mechanisms to mitigate illicit financial activities. Today, illicit cryptocurrency transactions are relatively rare,[7] and as the Treasury Action Plan rightfully acknowledges, there are fewer threats posed by illicit activities in the web3 ecosystem than in traditional finance.[8] Nevertheless, we recognize that bad actors still take advantage of blockchain technology to facilitate money laundering and other financial crimes, and that such actors, even if few in number, can have outsized effects on the industry as a whole. They stand in the way of broadscale adoption of blockchain technology and web3 and hinder responsible

[7] *See* Chainalysis Team, *Crypto Crime Trends for 2022: Illicit Transaction Activity Reaches All-Time High in Value, All-Time Low in Share of All Cryptocurrency Activity*, Chainalysis (Jan. 6, 2022), https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/ ("In fact, with the growth of legitimate cryptocurrency usage far outpacing the growth of criminal usage, illicit activity's share of cryptocurrency transaction volume has never been lower.").

[8] *See* U.S. Dep't of the Treasury's September 2022 "Action Plan to Address Illicit Financing Risks of Digital Assets" [hereinafter: "Treasury Action Plan"] at 2 ("While the use of virtual assets for money laundering remains far below the scale of fiat currency and more traditional assets by volume and value of transactions, virtual assets have been used to launder illicit proceeds as described in the NRAs."); 3 ("The size and scope of drug proceeds generated on the darknet and laundered via virtual assets, however, remain low in comparison to cash-based retail street sales."); 4 ("[Terrorism financing] cases are still less prevalent than those involving traditional financial assets.").

actors, like our portfolio companies, from advancing the industry. It is for these reasons that we appreciate Treasury's efforts to identify and mitigate illicit crypto risks, and we support appropriately tailored regulations as described below.

1. Privacy-Preserving Technologies Can Mitigate Illicit Finance Risks

The current architectures of most existing blockchains rely on transaction transparency to promote trust, but this default transparency and lack of privacy increases the risk of consumer harm by permitting other blockchain users to view the transaction history and holdings of any wallet holder. Indeed, modern blockchain analytics practices have shown that heuristic analysis of user interactions can be used to pierce the pseudonymous characteristics of blockchains, and anyone who transacts with a wallet holder may effectively be able to see their entire financial profile. Consequently, although it provides a net benefit in law enforcement's ability to trace illicit financial activity, transaction transparency makes users of blockchain technologies particularly vulnerable to fraud, social engineering, and theft of assets by bad actors, as well as the inchoate harm caused by revealing sensitive financial data to third parties.

Privacy-preserving technologies are a key emerging innovation in the blockchain ecosystem, and current research suggests that, with the proper design, market participants can build and implement them in a way that mitigates financial risks. This is important because, as discussed below, privacy-preserving technologies play a critical role in protecting American citizens from unwanted surveillance by American adversaries as well as from attacks by cybercriminals. But, we also appreciate the government's interest in preventing bad actors from using these technologies to launder money and engage in financial crimes.[9] We believe that technological developments in the industry address these concerns, and that the government need not compromise on deterring criminals in order for the public to realize the benefits of and rights to financial privacy.

[9] *Id.* at 3, 4, 5.

First, what are the national security benefits of privacy-preserving technologies? To understand the benefits, it is important to realize that on most public blockchains, all of a person's digital assets and transactions are available for anyone to see, including adversaries of the United States, like China, Iran, Russia, and Venezuela, as well as non-state actor cybercriminals. While a person transacting on a public blockchain does have some degree of privacy protection because of the pseudonymity of wallet addresses, as mentioned above, data analytics have become increasingly good at surmounting pseudonymity.[10] Accordingly, without the privacy afforded by enhanced layer-1 blockchains, mixing services, or other technologies, our adversaries could use surveillance networks to monitor our citizens through their blockchain transactions. Privacy-preserving technologies are, therefore, a crucial line of defense against such surveillance.[11]

Importantly, zero-knowledge proofs, the technical methodology that underlies many privacy-preserving products and services, can be designed and used to mitigate illicit finance and national security risks.[12] Current research suggests that there are a number of possible methods for privacy-enhancing products and services to mitigate risk, including, but not limited to: (1) *deposit screening* to prevent deposits of assets coming from sanctioned persons or wallets; (2) *withdrawal screening* to prevent withdrawals from sanctioned addresses or addresses associated with illegal activity; (3) *voluntary selective de-anonymization*, which provides persons who believe that they have been erroneously added to a sanctions list with the option to de-anonymize the details of their transaction to selected or designated parties; and (4) *involuntary selective*

[10] *See* Justin Sherman, *Big Data May Not Know Your Name. But It Knows Everything Else*, Wired (Dec. 19, 2021), https://www.wired.com/story/big-data-may-not-know-your-name-but-it-knows-everything-else/.

[11] Iron Fish, a layer-1 blockchain that provides privacy guarantees on transactions executed on the network, elaborates extensively on the national security benefits of privacy-preserving technologies in its comment letter response to the Request. *See* Craig Timm, *The Importance of Responsible Privacy in Digital Assets*, Iron Fish (Oct. 6, 2022), https://downloads.regulations.gov/TREAS-DO-2022-0018-0014/attachment_1.pdf. a16z Crypto is an investor in Iron Fish. Ali Yahya, *Investing in Iron Fish*, Andreessen Horowitz (Nov. 30, 2021), https://a16z.com/2021/11/30/investing-in-iron-fish/. A list of investments made by funds managed by a16z is available at https://a16z.com/investments/.

[12] Zero-knowledge proofs enable private transactions on a public blockchain. At its core, a zero-knowledge proof is a way for one party, called a "prover," to convince another party, a "verifier," that a certain statement is true, while revealing nothing about the underlying data that makes the statement true.

de-anonymization, which involves a private-key-sharing arrangement between a gatekeeper entity (like a non-profit or other trusted organization) and the government, where the gatekeeper entity evaluates requests from the government to use the private keys to de-anonymize wallet addresses.[13] We believe that methodologies like these may be used in a myriad of ways to provide new solutions for deterring crime, enforcing economic sanctions, and also preventing our adversaries from surveilling American citizens or using the blockchain ecosystem to steal or launder funds.

2. Regulating Web3 Applications, Not Protocols

As with privacy-preserving technologies, the American public can also benefit from DeFi markets without compromise on illicit activity. While blockchain technology's inherent transparency has an important initial role to play in exposing on-chain illicit activity, we also appreciate that transparency is not always enough to stymie bad actors. For this reason, we suggest pairing the transparency of DeFi markets with an appropriately tailored framework that focuses on regulating web3 applications, not protocols, as a potential solution.

As a threshold matter, it bears emphasizing that DeFi protocols are — by design — extremely transparent. DeFi protocols use cryptocurrencies and transparent smart contracts that are publicly available on the blockchain ledger for anyone to inspect and audit.[14] They provide real-time disclosures of price and quantity for transactions, as well as unique identifiers of traders and investors in the market.[15] For example, Compound,[16] a popular DeFi lending

[13] For more information on mitigation methodologies using zero-knowledge proofs, *see* Dan Boneh et al., *Privacy-Protecting Regulatory Solutions Using Zero-Knowledge Proofs* (pending publication Nov. 2022); *see also* Shlomit Azgad-Tromer et al., *We can finally reconcile privacy and compliance in crypto. Here are the new technologies that will protect user data and stop illicit transactions*, Fortune (Oct. 28, 2022), https://fortune.com/2022/10/28/finally-reconcile-privacy-compliance-crypto-new-technology-celsius-user-data-leak-illicit-transactions-crypto-tromer-ramaswamy/.

[14] *See Decentralized finance (DeFi)*, Ethereum, https://ethereum.org/en/defi/ (last updated Oct. 31, 2022).

[15] 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.

[16] a16z Crypto is an investor in Compound.

protocol, has a transparent, immutable, and publicly inspectable ledger of all historical transactions, including borrowing and lending.[17] Traditional financial markets, in contrast, are opaque.[18] The traditional lending market, for instance, is typically bilateral with no real-time price or quantity disclosures. Accordingly, given the transparency of DeFi markets, it is comparatively easy for the government to track illicit activity. And it is precisely DeFi's transparency that has allowed market observers to estimate, with a high degree of accuracy, that the amount laundered through DeFi protocols in 2021 is somewhere between 100 and 250 times *less* than the total figure laundered in the traditional markets.[19]

That said, as noted above, appropriately tailored regulations may be necessary where the inherent transparency of DeFi is not enough to deter bad actors. To that end, we believe that such a framework would involve the regulation of the applications, or onboarding access points to protocols, not the protocols themselves, which is an approach that is consistent with how the United States has historically regulated the Internet. This distinction — between applications and protocols — is crucial. Web3 protocols are open-source, decentralized, autonomous and standardized, and censorship resistant, and therefore, cannot incorporate subjective determinations that traditional finance regulations sometimes require. Businesses and developers of web3 applications do not have the same constraints. They can comply with regulations and design flexible 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]

---

[17] *See* Robert Leshner & Geoffrey Hayes, *Compound: The Money Market Protocol*, Compound (Feb. 2019), https://compound.finance/documents/Compound.Whitepaper.pdf.

[18] Traditional financial markets also include centralized financial services companies that hold, transact, or lend cryptocurrencies. For example, bankrupt crypto lender Celsius did not process transactions transparently on-chain, in contrast to decentralized web3 protocols like Compound. *See* BV Crypto, *Importance of Transparency: Celsius*, Medium (July 29, 2022), https://medium.com/@BV_Crypto/importance-of-transparency-celsius-55fbe2655233.

[19] Michael Karbouris, *The DeFi Financial Crime Arms Race*, CoinDesk (Sept. 27, 2022), https://www.coindesk.com/layer2/2022/09/27/the-defi-financial-crime-arms-race/.

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

We also believe that the principle of regulating applications, and not protocols, is important to ensuring that the United States remains the leader when it comes to the international financial system. Adoption of a regulatory framework that captures the software infrastructure that fuels the web3 ecosystem, rather than the applications which operate as intermediaries, is very likely to push DeFi innovation and businesses overseas.[21] Without this U.S. leadership and supervision, we are concerned that our adversaries, who are actively working on competing systems, may fill the void — posing a grave risk to our dominant position in international markets. The United States 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.

3. Treasury Can Enforce Existing Laws Against Illicit Finance Facilitators

We believe that noncompliance poses the greatest illicit finance risk in the blockchain industry, and Treasury is well positioned to use its existing authorities to address AML/CFT compliance failures with regulations already on the books. These existing legal and regulatory frameworks for financial institutions and money services businesses that offer fiat on- and off-ramps for the blockchain ecosystem provide sufficient safeguards to mitigate illicit finance risks in the crypto markets effectively, and technological developments in the industry have made compliance with these frameworks easier.[22]

It is no secret that the vast majority of criminal activity involving cryptocurrency still requires bad actors to convert funds to fiat currency in order to liquidate their proceeds. These cybercriminals and state actors avoid those exchanges that meet compliance obligations, such as

[21] 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.

[22] *See* Paul Grewal, *Coinbase Global Inc.'s Response to Treasury Request for Comment*, at 2–5 (Oct. 31, 2022), https://downloads.regulations.gov/TREAS-DO-2022-0018-0024/attachment_1.pdf.

performing KYC on account holders, filing suspicious activity reports, and freezing illicit funds, in favor of exchanges that fail to implement the same controls.[23] Treasury, the Department of Justice ("DOJ"), and the Financial Action Task Force ("FATF") have already highlighted the threats posed by noncompliant exchanges.[24] While it is encouraging that a growing number of countries are imposing AML obligations on service providers in their jurisdictions, there are still large gaps in global enforcement efforts.[28] Publicly available information demonstrates that illicit actors continue to use exchanges that take advantage of these gaps by engaging in jurisdictional arbitrage.[25] Some of these noncompliant exchanges have provided services to global customers unchecked for years, operating with weak or non-existent AML controls, and leaving businesses that operate responsibly with no expectation that regulators or law enforcement will ever hold them accountable. In addition to leaving the door open for illicit actors to realize their profits and other nefarious goals, failure to bring timely enforcement actions gives these noncompliant exchanges a competitive edge over those following the rules.

Thus, web3 businesses can be most successful in an environment where consumers and the American economy are protected from illicit finance risks, and we believe that FinCEN and

---

[23] U.S. Dep't of Justice, *The Report of the Attorney General Pursuant to Section 5(b)(iii) of Executive Order 14607: The Role of Law Enforcement in Detecting, Investigating, and Prosecuting Criminal Activity Related Digital Assets*, at 7 (Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download ("DOJ Digital Assets Report") (cautioning that "criminals continue to take advantage of noncompliant actors … including noncompliant cryptocurrency exchanges … to exchange their cryptocurrency for cash or other digital assets without facing rigorous [AML] scrutiny.").

[24] Treasury Action Plan, at 13–14 (identifying "non-compliant VASPs used to launder or cash out illicit funds [as a] primary concern."); FATF, *Second 12-Month Review Of The Revised FATF Standards On Virtual Assets And Virtual Asset Service Providers*, at ¶ 73 (July 2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (warning that illicit actors are taking advantage of poor screening processes at noncompliant VASPs); DOJ Digital Assets Report at 7.

[25] But, Treasury can enforce against businesses legally or physically located outside of the U.S. *See* 31 C.F.R. § 1010.100(ff); *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001, at 12 (May 9, 2019) ("FinCEN 2019 Guidance") (emphasizing that the BSA's "requirements apply equally to domestic and foreign-located [crypto] money transmitters doing business in whole or in substantial part within the United States, even if the foreign-located entity has no physical presence in the United States.").

the DOJ have sufficient enforcement authorities necessary to disincentivize noncompliance and create a space where lawful and responsible innovation can thrive.

4. NFTs Have Unique Characteristics That Can Mitigate Illicit Finance Risks

Newer to the web3 ecosystem are NFTs. NFTs are unique blockchain-based records of ownership that can be associated with different files or media. They can be thought of as digital building blocks in the web3 ecosystem. Many NFTs today are associated with digital art, profile pictures, or digital items for use in a video game. But this is just the beginning of use cases for NFTs. For example, NFTs are already being used for access to real-life events, and we are beginning to see non-transferable NFTs for records such as academic credentials, as well as governments beginning to explore the use of non-transferable NFTs for birth, death, and marriage certificates.[26]

Compared to more established crypto assets, NFTs appear to be less susceptible to money laundering and other financial crimes.[27] Among the reasons for this is that individual NFTs are unique (hence, "non-fungible") and have individual token IDs that are linked to the wallet address of their owners. Additionally, each NFT's metadata is stored on the blockchain and contains information about the NFT, such as token ID, a description, various attributes of the NFT, and a link to the media or item connected to that token. These characteristics make it easier to trace NFTs across the blockchain ecosystem and identify suspicious patterns of behavior. NFT metadata can also be used as additional clues to evaluate whether an NFT presents a higher risk of illicit finance or national security risk, as the content of the NFT

[26] *See* CA SB 786 (2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220SB786.
[27] *See* Chainalysis Team, *Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class*, Chainalysis (Feb. 2, 2022) (stating "NFT money laundering activity is small but visible"), https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/.

metadata can, for example, reveal that the NFT may be expressing support for a terrorist organization.[28]

The uniqueness and traceability of NFTs also makes it easier for platforms to identify NFTs that may be held by bad actors or that are the proceeds of crime and take action accordingly. For example, OpenSea,[29] an NFT marketplace, has Terms of Service that allow it to remove from view or prevent interaction with an NFT on the platform or to disable accounts in the event that OpenSea's rules are violated.[30] OpenSea has also leveraged the unique nature of NFTs to develop proactive automated mechanisms to try to prevent and deter criminal activity.[31]

For these reasons, it is critical that any regulatory framework for NFTs acknowledge and account for their distinct features. A regulatory framework that does not account for such distinct features could jeopardize powerful NFT use cases that are just beginning to emerge. Any framework should also consider how the nature of NFTs, combined with innovation in the blockchain space, can allow even small companies to leverage new technology — such as zero-knowledge proofs — and build on cross-industry and private-public sector collaboration to help identify and combat illicit finance, without presenting unnecessary privacy and security risks.

5. Supporting Cybersecurity-Focused Web3 Entities

Hacks perpetrated by bad actors against web3 companies pose a serious risk to the blockchain ecosystem. Not only do such attacks hinder responsible actors from advancing the industry, they also regularly result in the laundering of money for the benefit of adversaries of

[28] Jex Exmundo, *Isis is Minting Propaganda: When NFTs Put Lives on the Line*, NFT Now (Sept. 5, 2022), https://nftnow.com/news/isis-is-minting-propaganda-when-nfts-put-lives-on-the-line/.
[29] OpenSea is an NFT marketplace that offers NFTs across the following categories: domain names, music, photography, sports, trading cards, art, collectibles, utility, and virtual worlds. *See generally* https://opensea.io/ (last visited Nov. 1, 2022). a16z Crypto is an investor in OpenSea.
[30] OpenSea Terms of Service, Section 6, https://opensea.io/tos.
[31] *See* Saurabh Sharma, *Our Efforts to Prevent NFT Theft*, OpenSea (Nov. 2, 2022), https://opensea.io/blog/announcements/our-efforts-to-prevent-nft-theft.

the United States. Like Treasury and the Biden administration, we are deeply concerned about this important issue and committed to helping resolve it, and we suggest that policymakers also consider how, or to what extent, the government can play a role in incentivizing entities that create technologies to make the blockchain and web3 ecosystems more secure.

At a16z, our investments reflect the firm's commitment to securing the web3 ecosystem. We previously led a $23 million fundraising round in Forta, which is a real-time detection network for security and operational monitoring of blockchain activity.[32] To safeguard the ecosystem, the Forta Network runs detection bots to monitor for anomalous transactions, protocol attacks, and other things, which is useful for both managing and preventing attacks.[33] Aave, Compound, Instadapp, Lido, and MakerDAO[34] — the largest DeFi protocols — leverage Forta for security and operational monitoring, and the total value monitored by the Forta Network is more than $35 billion.

We also previously led a $34 million fundraising round for Spruce, a decentralized digital identity web3 startup.[35] Spruce builds open-source tools that help users collect, control, and own their data across the Internet. These tools help combat fraud by, for instance, allowing individuals to prove ownership over their social media accounts, websites, and other blockchain addresses.[36] Notably, Spruce's overarching mission — to give users more control over their digital identity — aligns with the outlook of numerous government regulators. The Federal Deposit Insurance Corporation has noted that digital identity proofing is "a foundational element to enable digital financial services to function properly,"[37] and more recently, Financial Crimes Enforcement Network Acting Deputy Director, Jimmy Kirby, stated that cryptographically stored

---

[32] Alex Wilhelm, *Forta Launches With $23M to Bring Better Security to Smart Contracts*, TechCrunch (Sept. 30, 2021), https://techcrunch.com/2021/09/30/forta-launches-with-23m-to-bring-better-security-to-smart-contracts/.
[33] *See How Forta Works*, Forta Network, https://docs.forta.network/en/latest/how-forta-works/.
[34] a16z Crypto is an investor in Compound, Lido, and MakerDAO.
[35] *See Spruce Raises $34M to Unbundle the Login for a User-Controlled Web*, Spruce (Apr. 20, 2022), https://blog.spruceid.com/spruce-raises-34m-to-unbundle-the-login-for-a-user-controlled-web/.
[36] *See The Toolkit for Decentralized Identity*, Spruce (2021), https://spruceid.com/spruceid.
[37] Fed. Deposit Ins. Corp., Financial Institution Letter, FIL-04-2022, FDIC and FinCEN Launch Digital Identity Tech Sprint (Jan. 11, 2021), https://www.fdic.gov/news/financial-institution-letters/2022/fil22004.html.

identity evidence "offers a high degree of potential to foster innovation."[38] Companies like Spruce will, therefore, help fulfill important government goals.

III. Conclusion

a16z greatly appreciates the opportunity to provide comments on these important matters. We support the goals of the Biden administration and Treasury in promoting responsible innovation and growth of the digital asset sector. As outlined in Executive Order 14067 (Ensuring Responsible Development of Digital Assets), issued by President Biden earlier this year, "The United States has an interest in ensuring that it remains at the forefront of responsible development and design of digital assets and the technology that underpins new forms of payments and capital flows in the international financial system…" We believe it is critically important that policy leaders in the government thoughtfully regulate blockchain technology, as it is rapidly becoming a key pillar of the financial system.

[38] Jimmy Kirby, Acting Deputy Director, Fin. Crimes Enf't Network, Prepared Remarks at the 2022 Federal Identity Forum & Exposition (FedID) (Sept. 7, 2022), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-acting-deputy-director-jimmy-kirby-during-2022-federal.

We view this comment letter as part of an ongoing dialogue between the public and private sectors, and a16z looks forward to continued engagement on these issues.

Respectfully submitted,

Jai Ramaswamy, Chief Legal Officer
a16z

Scott Walker, Chief Compliance Officer
a16z

Michele R. Korver, Head of Regulatory
a16z Crypto

Miles Jennings, General Counsel
a16z Crypto