

April 29, 2023

BY E-MAIL

Future regulatory regime for cryptoassets – consultation
Payments and Fintech
HM Treasury
1 Horse Guards Road
SW1A 2HQ

Re: Future financial services regulatory regime for cryptoassets – Consultation and call for evidence

To whom it may concern,

We greatly appreciate this opportunity to reply to the consultation and call for evidence, entitled “Future financial services regulatory regime for cryptoassets” (the “Consultation”), issued by HM Treasury (the “Treasury”) on February 1, 2023. 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 Treasury 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 decentralised social networks, identity management, enterprise solutions, financial services, content creation, environmental protection, data storage, and many other sectors. As an industry leader, we have also assisted domestic and international regulators and officials with education around the unique attributes of decentralised systems, as well as the development of clear and robust regulatory frameworks that are appropriately calibrated to those attributes. We hope to channel our industry observations in providing helpful feedback to the Consultation.

As a preliminary matter, we applaud the Consultation’s core design principle of “same risk, same regulatory outcome” for regulating the cryptoasset sector. In particular, it is encouraging that the Treasury’s interpretation of this principle recognises that it does not mean it will be appropriate to apply exactly the same form of regulation in all cases to achieve the same regulatory outcome, and that determining what regulation is appropriate to achieve the same regulatory outcome demands an assessment of whether relevant technologies and the ways they are used give rise to the same or additional risks or mitigate certain risks. The benefit of this approach is that it ought to guard against a singular focus on activities, 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, the decentralisation made possible by blockchain technology can eliminate certain risks associated with traditional business activities.

In this response letter, we therefore focus on what we see as the key considerations regulators must take into account if seeking to effectively regulate certain critical elements of the web3 ecosystem in a way that preserves the benefits of web3 technology and protects the future of the Internet, while reducing the risks of illicit activity and consumer harm. In particular, we focus on how decentralisation should influence the regulation of cryptoasset transactions and decentralised finance (“DeFi”). In regards to the regulation of cryptoasset transactions, we explain how cryptoassets have varying risk profiles, how decentralisation can reduce or eliminate risks associated with cryptoassets, why the dissemination of cryptoassets is necessary to achieve decentralisation and how consumers can be sufficiently protected in cryptoasset transactions. In regards to DeFi, we explain that although DeFi may resemble traditional finance and centralised crypto finance (“CeFi”) in terms of the services offered, it involves very different risk profiles unique to its structures. Given the unique risks of these products

and services, we believe that a tailored regulatory framework should be applied to oversee DeFi, rather than extending existing regulations under a “one-size-fits-all” approach. We also offer some insight into how web3 protocols (including DeFi protocols) typically become decentralised in practice and how regulation can ensure that such protocols are not disproportionately burdened by regulation that is not appropriately suited to these kinds of activities.

This response letter is divided into five parts: *First*, we provide a brief overview of a16z. *Second*, we provide an explanation of our vision for web3 and the importance of decentralisation. *Third*, we discuss the critical importance of developing a regulatory framework for cryptoasset transactions that will position the UK as the world’s web3 centre. *Fourth*, we discuss the differences between CeFi and DeFi, and how an appropriately tailored regulatory framework for DeFi should involve regulating web3 applications, not web3 protocols (“regulate businesses, not software”). *Lastly*, we provide comments in response to some of the specific questions included in the Consultation, focusing on those which we see as most relevant to DeFi and web3 more broadly.

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, with over \$7.6 billion for our crypto 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, decentralised applications and finance, blockchains, cryptoassets, and decentralised autonomous organisations. 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.

Within web3, we primarily invest in companies using blockchain technology to develop protocols that will give the Internet new native functionality – Internet infrastructure that millions of people will be able to build on top of to launch their own Internet businesses. To that end, we take a long-term view with respect to all of our investments, and our funds typically have a 10-year time horizon. We do not speculate in short-term cryptoasset price fluctuations and our focus is instead on empowering entrepreneurs to build robust and rich ecosystems that will benefit billions of people.

II. Web3 and Decentralisation

Over the past three decades, no technology has impacted the lives of the British people more than the Internet. But, just like any technology, the ways that individuals interact with the Internet have changed over time. The Internet can be viewed in three distinct eras: web1, web2, and web3. Each era brought its own new utility to consumers: the ability to read, the ability to write, and now the ability to own. In particular:

- **Web1 - Read (1990 - 2005).** The key feature of web1 was that it was governed by free and open software, commonly referred to as open protocols. Open protocols are not owned by an individual or a company and operate like public utilities. Users of the early Internet were frequently met with open protocol acronyms like HTTP or SMTP – the foundational code for web access / websites and email, respectively. These protocols served as base layer utilities, and their open nature allowed companies like AOL and Netscape to offer easy-to-use services built on top of these protocols. The hallmark of this era of the Internet was the ability to take offline readable material and put it online. Most Internet users of this era were only able to consume information but were limited in their ability to interact. This was the “read” era.
- **Web2 - Read, Write (2005 - 2020).** Building off of the core open protocols used in web1, entrepreneurs and developers created new Internet technology to enable people to interact and collaborate with one another online. For the first time, users could be interactive online. Instead of simply reading the *Financial Times* on a web browser, individuals could now create websites like Facebook, Twitter, and YouTube, where anyone could be their own publisher or broadcaster. This is the “read and write” era of the Internet. These advancements helped accelerate and democratise access to information and communities. In the early days of web2, competition thrived. But over time, participation and economic power consolidated with a handful of large companies. Today, millions of people have built successful businesses based on the access these centralised organisations provide (influencers through Instagram, craftspeople through Etsy, entertainers through YouTube, for example), but most of the economic value flows to the centralised platform and not the small business / user. These entities can also choose to deplatform an individual user at any time or censor / promote content. The Internet went from open and buildable to closed and controlled.
- **Web3 - Read, Write, Own (2020 - Present).** We are now at the very beginning of the web3 era, which combines the easy-to-use “read and write” functionality of web2 with the ability for users, rather than centralised companies, to, for the most part, own the Internet. In particular, web3 technology enables a new paradigm featuring “trustless computation,” which removes the need to rely on a centralised entity to navigate the web and databases. This makes it possible to develop more complex and sophisticated protocols that offer the functionality of web2 but that can also be owned by users. In addition, it enables users and builders to own their contributions to networks, their intellectual property, and their digital identities, which ownership is denoted in cryptoassets. For example, the current business model for Twitter provides next to no economic value for individuals who publish on the platform. All of the value accrues to the company, which has the ability to decide who can participate. In web3, a high-performing user or post accrues most of the economic value, and the community of users, through a public voting process and open source code, decides who can participate and post. This structure fixes the core problem of web2 centralisation, where the value is accumulated by one company, and the company ends up fighting its own users and partners. This is the “read, write, and own” era.

Decentralisation is the critical feature of web3 systems that enables this paradigm shift and is therefore what will drive the creation of a democratised Internet. This will provide several significant benefits, including:

- **Promoting Competition** - Decentralisation enables blockchain networks to be credibly neutral¹ and composable.² This ensures that they function like public infrastructure and makes them attractive to build on top of. This then lowers the barrier to entry for anyone wanting to

¹ See Vitalik Buterin, *Credible Neutrality As A Guiding Principle*, Nakamoto (Jan. 3, 2020), <https://nakamoto.com/credible-neutrality/>.

² *Smart Contract Composability*, Ethereum, <https://ethereum.org/en/developers/docs/smart-contracts/composability/> (last updated Aug. 15, 2022).

build an Internet business, as it provides Internet infrastructure upon which such businesses can be built. As a result, decentralisation will promote competition.

- **Safeguards Freedoms** - Decentralisation necessitates the broad distribution of control of blockchain networks among their stakeholders and ensures that the network effects of such systems accrue to such stakeholders, not just the companies that created them. By limiting the power that can accrue to companies in this manner, decentralisation limits corporate power to gatekeep, censor, or otherwise infringe individual liberty. As a result, decentralisation has the power to safeguard user freedoms.
- **Rewards Stakeholders** - Decentralisation enables the design of systems that prioritise stakeholder capitalism – systems that are designed to more equitably serve the interests of all stakeholders, rather than a certain subset of stakeholders. For example, web3 systems can be designed to more equitably reward users and contributors, rather than being designed to maximise value of shareholders, as is the case with the corporate networks of web2.

Given the potential benefits decentralisation enables, it is critical that policymakers and regulators develop a more uniform understanding of decentralisation and the various types of decentralisation that might apply to a web3 system.³ For much of the blockchain industry’s development, concepts of decentralisation have been focused on decentralisation from a perspective of security – namely, is a system sufficiently decentralised such that it is not vulnerable to attack by third parties. For blockchain protocols, this is an exceedingly challenging problem and is one that requires a balancing of several competing forces. Meanwhile, for smart contract protocols (software programs that are deployed and operated on blockchains), this type of decentralisation can be achieved relatively quickly and easily, by making the smart contracts immutable (i.e. software that cannot be controlled or modified by anyone once deployed). The use of digital assets by these systems further complicates the decentralisation challenge, as it adds economic forces and legal regimes to the list of necessary considerations.

Ultimately, any regulatory framework applicable to web3 must include a principles-based analysis that considers decentralisation, focusing on whether the decentralisation present in a web3 system obviates the risks that a specific regulation applicable to such system is intended to address. If the risk is negated, then the application of such regulation to the web3 system is unnecessary. Further, any regulatory framework should seek to incentivise decentralisation in order to maximise the potential public benefit arising from web3.

For purposes hereof, we will now discuss the impact decentralisation has on risks associated with cryptoasset transactions and a specific type of web3 protocol (DeFi protocols), and how that should influence the UK’s approach to regulating web3.

III. Regulating Cryptoasset Transactions

Cryptoassets can take on a number of different qualities and characteristics that impact the inherent risks associated with such assets. In certain cases, the value of a cryptoasset may be entirely dependent on the managerial efforts of a small group of individuals, which could lead to a high likelihood of significant information asymmetries, and warrant the application of a regulatory framework with robust consumer and investor protections. In other cases, the value of a cryptoasset may be entirely dependent on market forces and user demand for the asset’s underlying protocol, and strong consumer / investor protection may be less necessary. As a result, a “one-size-fits-all” approach to the regulation of cryptoasset transactions would not be consistent with the Treasury’s core design principle of “same risk, same regulatory outcome.” Given the difference in risk profiles and because the broad dissemination of decentralised cryptoassets is both critical to spurring innovation in web3 and provides

³ For a more extensive discussion of decentralisation in the context of web3, see Miles Jennings, *Principles & Models of Web3 Decentralisation*, Andreessen Horowitz (Apr. 2022), https://a16z.com/wp-content/uploads/2022/04/principles-and-models-of-decentralisation_miles-jennings_a16zcrypto.pdf.

significant public benefit, a more nuanced approach to the regulation of cryptoasset transactions is worth consideration.

Indeed, while we are generally supportive of the Treasury’s proposal to expand the list of "specified investments" to cover cryptoassets that are not already regulated, the proposal to expand the list of cryptoasset activities within the regulatory perimeter, and the various proposals relating to cryptoasset issuances, offerings and disclosures, it is critical that the implementation of these proposals does not result in unnecessary impediments to the dissemination of cryptoassets by web3 projects attempting to decentralise. Any overly broad restrictions of such activity could jeopardise the UK’s ability to realise its vision of becoming a “web3 centre”. As such, in this section we provide information about how cryptoassets are currently disseminated, the specific types of transactions that are most important for decentralisation (and therefore the most important to be unrestricted) and why these present lower risks to consumers (allowing for an appropriate policy balance to be struck between consumer protection and encouraging innovation in these cases).

A. Decentralised and Centralised Cryptoassets

Decentralisation is the primary characteristic that is relevant for determining the risk profile of a given cryptoasset. Specifically, decentralised cryptoassets primarily derive their value from decentralised sources, such as market forces, user demand for the underlying protocol and the number of developers building on top of the protocol, rather than the managerial efforts of a single development team. In other words, they are inherently trustless (in the sense that no single group of individuals possesses classic “insider information” that could have a material effect on asset prices). These assets are typically (i) utilised in the functioning of a decentralised web3 protocol (“utility cryptoassets”), (ii) provide holders with governance rights with respect to the protocol (“governance cryptoassets”) and / or (iii) provide holders with a non-contractual claim to the protocol’s assets. Given the transparent nature of blockchains, all relevant information about these cryptoassets can typically be found on-chain, meaning that all potential holders of such assets have access to the information necessary to value and trade them on a level playing field.

Conversely, centralised cryptoassets primarily derive their value from centralised sources, such as the managerial efforts of a development team. In other words, they inherently involve trust. While these assets can provide the same utility and functionality as decentralised cryptoassets, they can also represent more traditional financial instruments like bonds or shares. Regardless, the presence of centralisation increases the risk that holders of such cryptoassets may be relying on the efforts of a management team to drive the value of their assets. Furthermore, this centralisation increases the likelihood that significant information asymmetries relating to the value of the centralised cryptoassets may arise, and therefore increases the risks that all potential holders of such cryptoassets are not equally situated with respect to their purchase and sale decisions.

As a result of the foregoing dynamic, the risks to consumers in cryptoasset transactions like primary issuances and secondary market transactions will vary significantly depending on whether the transactions involve decentralised or centralised cryptoassets. It is therefore critical that the UK develop a nuanced regulatory approach to cryptoasset transactions that allows for a principles-based analysis of decentralisation. This would then facilitate a regulatory approach that has a lighter touch for decentralised cryptoassets (where risks to consumers are lower) and a heavier hand for centralised cryptoassets (where risks to consumers are higher), thereby achieving the Treasury’s goals of focusing on regulatory outcomes and promoting innovation.

In the United States, the approach used to distinguish between decentralised and centralised cryptoassets is called the “Howey Test”, which was derived from case law that defined the term “investment contract” under the U.S. Securities Act of 1933. However, the application of this test has resulted in several significant challenges that the UK would do best to avoid, including:

- **Lingering Uncertainties** - The Howey Test is subjective and creates significant uncertainty as to which cryptoassets are securities under the test. The regulator responsible for administering

the test, the U.S. Securities and Exchange Commission (“SEC”), has not provided formal guidance on how to apply the Howey Test to cryptoassets since 2019, and has left many questions about the functioning of modern protocols unanswered. Without additional guidance, it is nearly impossible for legal practitioners in the United States to adequately advise clients as to whether a given cryptoasset is sufficiently decentralised and thereby not a security.

- **Difficult to Enforce** - The Howey Test is difficult to enforce, and its subjective nature has meant that the SEC needs to expend considerable resources in order to determine whether a given cryptoasset is decentralised. Bad actors have taken advantage of these uncertainties and the lack of uniform enforcement to harm consumers. For instance, there are numerous examples of builders creating protocols and launching cryptoassets that are falsely marketed as “decentralised” but in fact are centralised and involve trust. The lack of uniform enforcement also harms good actors in the industry who are therefore forced to compete on an unfair playing field.
- **Impractical to Apply** - The framework for the Howey Test put forward by the SEC in 2019 is also impractical to apply. Specifically, the framework provides that a transaction involving decentralised cryptoassets should not be treated as a securities transaction, but it does not address projects that decentralise (or recentralise) over time. In practice, a project could meet decentralisation thresholds one day and not another — without secondary market participants ever being able to assess the difference.
- **No Pathway for Progressive Decentralisation** - The SEC’s framework does not facilitate “progressive decentralisation”. As discussed further below, cryptoassets are a tool for achieving decentralisation, but the SEC’s framework necessitates that cryptoassets be decentralised in order to lawfully issue their digital assets. This can create a “chicken-or-the-egg” paradox for projects that need time and the ability to make use of a cryptoassets to increase their overall decentralisation.

Meanwhile, the SEC’s continued broad and sporadic application of the Howey Test to bring enforcement actions has resulted in significant uncertainty that incentivises regulatory arbitrage and has a severe economic drag on the entire web3 industry. This uncertainty and the lack of uniform enforcement has also created greater risk of asymmetrical information between developers and insiders (development company employees and investors) of a given project and users of such projects. As a result, the U.S. approach is not one that the UK should consider adopting.

Despite these challenges, we believe the UK can successfully adopt a principles-based approach to decentralisation that facilitates the broad dissemination of cryptoassets to drive web3 innovation in the UK while prioritising consumer protection in cryptoasset transactions.

B. Cryptoasset Transactions

Decentralisation is a spectrum, with some web3 businesses starting off centralised and transitioning toward a decentralised model. In the vast majority of cases, the decentralisation of a web3 protocol depends on the broad dissemination of decentralised cryptoassets native to the relevant protocol in various types of cryptoasset transactions (including, broad primary issuances not conducted as public sales, as well as limited issuances conducted for capital raising purposes and secondary transactions). In particular, broad dissemination is necessary to ensure that: (i) the performance of activities crucial to the functioning of the protocol (such as mining or other forms of validation) by a sufficient number of diverse actors can be properly incentivised; or (ii) decentralised governance models that rely on cryptoasset holder voting can be truly decentralised (by avoiding concentrations of voting power within small groups of cryptoasset holders), or both. As a result, any regulatory framework for web3 must seek to facilitate such dissemination – restrictions could act as impediments to web3 protocols decentralising and hinder innovation. Nevertheless, such facilitation must be balanced against the risks to consumers, which must be mitigated to the extent possible.

a. Background on Cryptoasset Dissemination

Prior to 2018-19, many traditional private limited companies developing blockchain projects (“Development Companies” or “DevCos”) sought to sell cryptoassets to the public via initial coin offerings (“ICOs”) as a means of facilitating a wide distribution of cryptoassets while also raising funds for further development of the project. In these types of transactions, the risks to consumers are readily apparent as the consumer is likely to reasonably rely on the managerial efforts of the DevCo to drive the value of the cryptoasset. As a result, the cryptoassets sold in these types of transactions are most likely to be centralised cryptoassets that warrant strong consumer protections similar to classic securities regulations. In this case, the extension of existing regulations applicable to other assets under a “one-size-fits-all” approach may be appropriate.

However, primary sales of cryptoassets by issuers to the public rarely happen anymore and are unlikely to become popular in the future. Instead, builders of web3 projects (either “Layer 1” blockchain protocols or “Layer 2” smart contract protocols deployed to blockchains) now typically form a DevCo and raise capital in private placements of their equity to institutional investors in order to fund the DevCo’s development activities. This tracks the well-trodden pathway of tech startups the world over. Once development of a web3 project is completed and the protocol under development is fully-functional⁴, the DevCo typically seeks to decentralise the protocol.

Decentralisation is a complex process that requires limiting the ability of any party to control the technical and economic elements of the protocol. The most likely source of technical control is the DevCo – if it retains sufficient power or flexibility to unilaterally change the functioning of the underlying protocol, then user assets could be at risk and the protocol would not be decentralised. However, third parties can also acquire control through various economic mechanisms. This risk can be greatly reduced by broadly disseminating the protocol’s cryptoassets. For example, the broad dissemination of cryptoassets could limit the ability of a party to manipulate the economics of a protocol in their favour, thereby limiting their ability to launch a 51% attack.⁵

The process of decentralisation also often includes setting up decentralised governance to administer, maintain and govern the affairs of the protocol. This decentralised governance can utilise “off-chain” voting (typically orchestrated by a foundation setup for the network) or on-chain cryptoasset-based voting mechanisms (typically orchestrated by a decentralised autonomous organisation (“DAO”)). These decentralised governance systems typically seek to establish consensus with respect to decisions relating to the underlying protocol, funding public goods and other projects that are beneficial to the protocol’s ecosystem and making decisions with respect to future development of the protocol. As described above, the broad dissemination of a protocol’s cryptoassets is critical to ensure that no individual or group can initiate a governance attack and take control of the protocol’s governance function.

The dissemination of cryptoassets by a DevCo is typically multifaceted. A DevCo will often issue cryptoassets for no or *de minimis* consideration to its employees as a reward for having developed its protocol and to its investors for having funded the development of its protocol. The remaining cryptoassets of a given protocol are then typically distributed for free to users of the protocol via “airdrops” and incentive-based rewards (such as rewards for liquidity mining, staking, validation, mining, or other service-based compensation), as well as to a foundation controlled by the decentralised

⁴ Necessitates that (1) a protocol is composed of source code that is publicly available and accessible and whose primary purpose cannot be materially altered or disabled by a single person or group of persons acting pursuant to an express or implied agreement, and is designed to prevent any such person or persons from amending or reversing transactions executed and recorded on the protocol; and (2) the protocol enables multiple participants to execute digital asset transactions in accordance with predetermined non-discretionary automated rules or algorithms.

⁵ See Griffin McShane, *What Is a 51% Attack*, CoinDesk (Oct 2021), <https://www.coindesk.com/learn/what-is-a-51-attack/>.

governance mechanism adopted by the protocol. DevCo’s employees and investors, the network users and any other recipients or acquirers of the cryptoassets make up the constituents of the decentralised governance mechanism.

b. Primary Transactions

While cryptoassets sold to the general public in fundraising transactions prior to the development of a given protocol may warrant regulatory treatment similar to that of other regulated investment activity (as discussed above), we believe a more agile regulatory framework is appropriate for cryptoassets that are airdropped with a view to decentralising a “fully-functional” protocol and cryptoassets that are disseminated as incentive-based rewards. Unlike cryptoassets sold prior to development of a protocol, cryptoassets distributed after a protocol is “fully-functional” for free (or on a *de minimis* basis) are significantly more likely to derive their value from the decentralised functioning of the protocol, and not from the ongoing efforts of the DevCo. Further, the recipients of such cryptoassets would have no contractual or legal right to the ongoing efforts of the DevCo. In other words, these cryptoassets look more like decentralised cryptoassets than centralised cryptoassets, and as a result, a more proportionate regulatory framework that does not impede broad dissemination is appropriate. Furthermore, because airdrops and incentive-based rewards effectively hand ownership of web3 infrastructure from the DevCo to the general public, there is significant public benefit in such behaviour and it should be incentivised under the UK’s regulatory framework.

c. Secondary Transactions

In addition, we believe that a more calibrated regulatory framework for secondary market transactions of freely distributed cryptoassets is warranted. A liquid secondary market provides several benefits to the protocol’s users and cryptoasset holders, including helping to facilitate the broad dissemination of the cryptoassets, enabling new users to acquire cryptoassets that may be necessary to use the protocol, allowing early adopters or ongoing network contributors to realise the value of their participation, and reducing volatility in the price of such protocol’s cryptoassets.

However, the existence of a secondary market also introduces risks that are not present with the free or *de minimis* primary transactions described above. In particular, as participants in such markets would be using their own capital to purchase a protocol’s cryptoassets, there is greater risk of such consumers experiencing losses, which is not present with the free or *de minimis* primary transactions. Furthermore, when a “fully-functional” protocol for a cryptoasset is in the process of decentralising, but not yet fully decentralised, there is greater risk of significant information asymmetries existing about the value of such cryptoasset. For instance, the DevCo associated with such protocol may be incentivised to give users the impression that they are contributing efforts that are driving the value of the cryptoasset, even where that may not be the case.

Given this dynamic, it may therefore be necessary to protect participants in such secondary markets and we note that the Treasury has proposed certain measures in the Consultation relating to listings and trading venues to provide such protection. However, we believe the Treasury should ensure that any obligations placed on issuers and trading venues relating to such protections do not impede the ability of issuers to decentralise the underlying protocol associated with any cryptoasset to be listed on a secondary market.

In order to achieve this, any regulatory framework adopted should focus on protecting consumers from the parties that would be most likely to possess asymmetric information about the value of the a cryptoasset listed on a secondary market (e.g. the protocol’s DevCo, its employees and investors). This could be accomplished through a robust disclosure regime (like the one for centralised cryptoassets discussed below) or by restricting the ability of such persons to trade the relevant cryptoasset until the point in time at which the cryptoasset has been decentralised. In the latter case, once the process of decentralisation was complete, the status of the cryptoasset as being decentralised could then be certified

by a regulated exchange or the relevant regulator based on the decentralisation principles adopted by the regulator.

The benefit of this construct is that it can significantly mitigate risks to consumers while effectively making the persons with the most power with respect to a given protocol and its cryptoassets (e.g. the DevCo, its employees and investors), the persons that are also most incentivised to pursue the protocol's and its cryptoasset's decentralisation.

C. Disclosure Requirements

The risks to consumers in any cryptoasset transaction can be partially mitigated through the adoption of a well-tailored disclosure regime, which should be part of the UK's regulatory framework. An issuer-centric disclosure regime is likely appropriate for centralised cryptoassets, given that their value is squarely based on the efforts of a management team. In such cases, the extension of existing disclosure regime obligations applicable to other assets under a "one-size-fits-all" approach may be appropriate. Some modifications may be necessary, however, such as disapplying any issuer-based disclosure regime after a protocol's cryptoassets become truly decentralised.

For decentralised cryptoassets, an issuer-centric disclosure regime does not make sense. For instance, the issuer's finances are irrelevant, as the cryptoassets have no claim them — they only have a right associated with the protocol. Decentralised cryptoasset holders rely on the operation of the protocol to generate value, rather than the efforts of the issuer to develop the protocol (as is the case with ICOs and cryptoasset sales conducted prior to the development of the protocol). Thus, any applicable disclosure requirements should be narrowly tailored and be capable of being satisfied with on-chain data. It is critical that any such disclosures be capable of being automated, otherwise the regulatory framework could effectively enforce an element of centralisation by requiring a centralised actor to be responsible for complying / procuring compliance with disclosure requirements.

D. Conclusion

Ultimately, it is critical that web3 companies be able to decentralise and be incentivised to do so within applicable regulatory frameworks. That decentralisation process includes both primary issuances of cryptoassets to the public for free (or on a *de minimis* basis) or in connection with incentive-based rewards, and regulatory frameworks must permit such cryptoassets to be trade on secondary markets, in each case, without inappropriate or unachievable obligations. Otherwise, there would be no way for a project to effectively decentralise since, as explained above, the process requires the wide dissemination of cryptoassets and no entity would be capable maintaining a licence without also jeopardising the project's overall decentralisation. That could substantially impede UK-based innovation, as the regulatory expense associated with issuing a cryptoasset would be prohibitive for companies and fatal for decentralised ecosystems. For instance, how would Ethereum, which has no centralised entity but which autonomously issues ETH to validators ever acquire or maintain a licence?

We discuss this further in relation to specific aspects of the Treasury's currently proposed regulatory regime in our comments in relation to specific questions in the Consultation in the next section of this response letter.

IV. Regulating DeFi

We commend the Treasury's proposed phased approach and applaud the Treasury's commitment to understanding further how DeFi works before introducing a regulatory framework for it. In our view, ensuring a proper understanding of DeFi at a granular level – and, in particular, its operational, organisational, and functional differences to traditional finance or CeFi – is essential for any authority seeking to develop an effective regulatory regime for DeFi. Taking the time to understand this novel and evolving sector before acting should also mitigate the risk that the regulatory regime would need to be fundamentally re-shaped later, with potentially costly consequences for the UK in the

meantime if a burdensome or uncertain regulatory environment were to dissuade DeFi projects and the broader web3 ecosystem from building and operating in the UK.

In this regard, it will be important to ensure that the regulatory framework for cryptoassets that is introduced now with the aim of addressing some of the more pressing policy objectives relating to CeFi (such as investor protection) does not inadvertently hamper the development of a burgeoning web3 and crypto ecosystem in the UK by imposing inapposite regulatory burdens on current and future decentralised ecosystems that would effectively prohibit web3 protocols or businesses from launching and operating in the UK. Accordingly, as we elaborate in this response letter, we think there are certain elements of the Treasury’s currently proposed regulatory regime where care should be taken to ensure that they do not apply to decentralised ecosystems (and persons performing certain crucial technology functions in relation to those ecosystems) or in circumstances that typically obtain in relation to web3 and DeFi protocols early in their lifecycle on the path to decentralisation.

A. DeFi

DeFi systems 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. 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 decentralisation provided by permissionless systems.⁶ 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 characterise 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 to trust that regulation will keep such intermediaries honest — a system that has failed too many times to count and that will never be able to be truly trustless. Further, 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 bespoke 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 or software. Businesses can comprehend and comply with jurisdictional regulations. Globally accessible software cannot.

B. CeFi Versus DeFi

a. 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.⁷ But CeFi and DeFi operate in fundamentally different ways, and it is

⁶ 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.”)

⁷ 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>.

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 “centralised” operations, complete with management teams and conflicts of interest, where users interact with third-party intermediaries to access crypto markets.⁸ 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 decentralised blockchain. Users can interact with these protocols directly, without intermediaries, to trade financial products in peer-to-peer transactions,⁹ 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.

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.¹⁰ For example, Compound,¹¹ a popular DeFi lending protocol, has a transparent, immutable, and publicly inspectable ledger of all historical transactions.¹² 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, including their utilisation of 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. The transparency underpinning DeFi can also mitigate contagion risks, as it decreases the ability for participants to take on opaque leveraged positions and encourages informed, community-driven risk management.

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,¹³ like Celsius Network and Voyager Digital, while truly decentralised DeFi protocols, like the Compound¹⁴ lending protocol and

⁸ *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/>.

⁹ *Decentralised finance (DeFi)*, Ethereum, <https://ethereum.org/en/defi/> (last updated Dec. 14, 2022)

¹⁰ 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.

¹¹ 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/>.

¹² See Robert Leshner & Geoffrey Hayes, *Compound: The Money Market Protocol*, Compound (Feb. 2019), <https://compound.finance/documents/Compound.Whitepaper.pdf>.

¹³ 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>.

¹⁴ Compound is a decentralised 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 collateral 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-collateralised to protect against price

the Uniswap exchange,¹⁵ have continued operating without interruption or compromise.¹⁶ 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. 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.¹⁷ In the world of DeFi, where traditional financial services are disintermediated, there are no intermediaries to trust. Accordingly, in DeFi, the decentralisation, 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.

C. A 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 centralised / 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.

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,¹⁸ and they are open-source, decentralised, autonomous,

fluctuations among the cryptocurrencies that serve as collateral. Another token within the Compound network is its governance token, known as “COMP,” the holders of which may vote on a limited set of protocol parameters, including which tokens may be deposited as collateral. See Leshner & Hayes, *supra* note 12.

¹⁵ 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 decentralised 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 market maker. More specifically, unlike centralised 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 cryptoassets 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 cryptoasset can “swap” their cryptoassets with tokens in the liquidity pools. There is a liquidity pool for each cryptoasset listed on the protocol, and an algorithm run by a computer calculates the price of each cryptoasset. See Ollie Leeche, *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/>.

¹⁶ Shai Bernstein & Scott Duke Kominers, *Why Decentralised Crypto Platforms Are Weathering the Crash*, Harv. Bus. Rev. (Dec. 7, 2022), <https://hbr.org/2022/12/why-decentralised-crypto-platforms-are-weathering-the-crash?ab=hero-main-text>.

¹⁷ See FTX, Celsius Network, Voyager Digital, 3AC, MF Global, Revco, Fannie Mae, Lehman Brothers, AIG, Long-Term Capital Management, and Bernie Madoff.

¹⁸ Lindsay X. Lin, *Deconstructing Decentralised Exchanges*, Stan. J. Blockchain L. & Pol’y (2015), <https://stanford-jblp.pubpub.org/pub/deconstructing-dex>; see also Fred Ehrsam, *Why Decentralised Exchange*

and censorship resistant. Of these characteristics, decentralisation and censorship resistance have particular regulatory and political significance.

- Decentralisation is a broad term that refers to multiple aspects of a blockchain, including political / legal decentralisation (because no one controls public blockchains) and architectural decentralisation (because there is no central point of failure from a technical perspective).¹⁹ As many regulators have noted, and as we note above, decentralisation is a spectrum, with some web3 businesses starting off centralised and transitioning toward a decentralised model. We have suggested that a “sufficiently” decentralised web3 entity exists where: (i) information regarding its operation is transparent and available to all (enabled by transparent blockchain ledgers); (ii) the protocol is composed of open source code and whose primary purpose cannot be materially altered or disabled by a single person or group of persons acting pursuant to an express or implied agreement, and whose design prevents any such person or persons from amending or reversing transactions executed and recorded on the blockchain; and (iii) public participants have the ability to access the protocol and execute digital asset transactions through such protocol in accordance with predetermined, non-discretionary automated rules / algorithms.
- Censorship resistance, like decentralisation, is a similarly broad term that describes the ability of almost anyone to use public blockchains, as well as the fact that no one can be kicked off of a public blockchain.²⁰ It also describes the fact that no one interacting with the blockchain is powerful enough to block transactions or prevent others who wish to validate blockchain transactions from joining the consensus network. Protocols must not have the ability to censor individuals or transactions. While the power to censor might appear attractive, such power jeopardises the credible neutrality and utility of protocols, including by making them susceptible to misuse by bad actors. For instance, a DAO having the power to alter a protocol to censor a user could sufficiently incentivise an individual to seek control of the DAO in order to censor their competitors. One can imagine that if the email protocol SMTP had the power to censor certain providers, that large email service providers like Google might seek to wield their influence to gain control of SMTP, and censor the email services of competitors like Microsoft or Apple. Furthermore, the ability of a given protocol to censor would jeopardise its autonomous nature, and would likely lead regulators from around the world to subject such protocol to numerous, conflicting regulatory schemes that would be impossible to comply with. And even if such compliance were possible, it would run counter to the Treasury’s objective of encouraging growth and innovation. 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, as discussed in the next section, applications accessing the SMTP protocol — Gmail for instance — could comply with various regulatory requirements or be responsive to regulatory information requests.

Because no one controls a decentralised protocol, a decentralised 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 programming. Further,

Protocols Matter, Medium (Sept. 27, 2017), <https://medium.com/@FEhrsam/why-decentralised-exchange-protocols-matter-58fb5e08b320>.

¹⁹ Vitalik Buterin, *The Meaning of Decentralisation*, Medium (Feb. 6, 2017), <https://medium.com/@VitalikButerin/the-meaning-of-decentralisation-a0c92b76a274>.

²⁰ 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.

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 often severely limit functionality updates.²¹

b. DeFi Applications

DeFi applications are products built on top of DeFi protocols that allow users to access the protocols. Importantly, they sometimes add an on-chain or off-chain order book database, and a graphic user interface (GUI) or APIs or both.²² 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 access points that minimise legal and regulatory risks. Still, for the reasons discussed above, wholesale application of CeFi regulations to DeFi applications—particularly those applications that do not provide intermediary-like services—would be inappropriate. We have written extensively about the “regulate apps, not protocols” principle, and we encourage the Treasury to review our findings, which can be found on our website.²³

c. 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,²⁴ 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.²⁵ DeFi is also making inroads in African countries, like Nigeria and Kenya.²⁶

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 jeopardise the benefits of DeFi for millions of people, and push protocol developers to jurisdictions with particularly loose regulatory frameworks. In this regard, we agree with the Treasury’s helpful statements in the Consultation that the objective is not to regulate the activity of developing software, and that a viable regulatory hook for DeFi may be centralised on and off ramps that facilitate access to DeFi (rather than other parts of the value chain that may not be practical to regulate, such as a truly decentralised protocol)²⁷.

²¹ See *The Uniswap Protocol*, <https://docs.uniswap.org/concepts/uniswap-protocol>.

²² See Lin, *supra* note 18.

²³ See Miles Jennings, *Regulate Web3 Apps, Not Protocols*, Andreessen Horowitz (Sept. 29, 2022), <https://a16zcrypto.com/web3-regulation-apps-not-protocols/>.

²⁴ See Anna Stone, *Why decentralised 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/decentralised-finance-a-leapfrog-technology-for-the-unbanked/>.

²⁵ 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/>.

²⁶ 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/>.

²⁷ And the current UK approach to regulation of both cryptoassets and payment services already reflects the principle that pure software/technology providers should not be captured by regulation. See Joint Money

If regulators were to impose subjective and potentially globally conflicting regulations — such as what may or may not be a security, commodity, or derivative of each — on web3 protocols, decentralisation 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 and applying disclosure requirements to such applications to ensure that users are aware of the risks of using them and their underlying protocols.

V. Comments in Relation to Specific Consultation Questions

Against the backdrop described above, overall we welcome the Treasury’s proposed approach to cryptoasset regulation set out in the Consultation.

We include in this section our comments in response to specific questions in the Consultation.

Laundrying Steering Group, *Guidance For The UK Financial Sector Part II: Sectoral Guidance*, at 22.12, 22.16, 22.25 and 22.26 (Jun. 2020 amended Jul. 2022), https://www.jmlsg.org.uk/wp-content/uploads/2022/09/JMLSG-Part-II_July-2022.pdf; see also the exclusion for technical service providers who do not come into possession of funds set out in paragraph 2(j) of Part 2 of Schedule 1 to the Payment Services Regulations 2017, <https://www.legislation.gov.uk/ukxi/2017/752/schedule/1/part/2>.

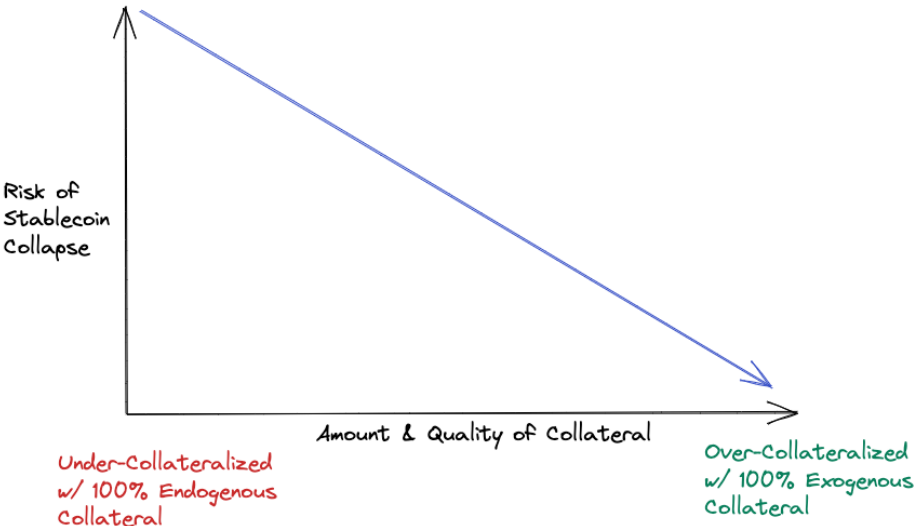
| | Consultation Questions | a16z Comments |
|---|---|---|
| 1 | <p>Do you agree with HM Treasury’s proposal to expand the list of “specified investments” to include cryptoassets? If not, then please specify why.</p> | <ul style="list-style-type: none"> ● In general, we recognise that expanding the existing list of specified investments to apply to all cryptoassets, rather than the scope of the new regulatory regime depending instead / also on distinctions between different kinds of cryptoassets, provides certainty with respect to the asset scope of the proposed new regime. However, this obviously makes whether or not a person is regarded as carrying on certain activities in relation to cryptoassets by way of business the determining factor for whether regulation will apply. ● If this approach is taken, then in order for the UK to realise its vision to become a “web3 centre”, we would strongly recommend that the activities captured by the new regime are appropriately limited in scope, or that specific express exclusions from relevant activities are included to ensure that: <ul style="list-style-type: none"> ○ decentralised protocols and the acts of publishing, developing, maintaining or administering software are not subject to regulation. This could be achieved by the inclusion of a general exclusion for protocols that meet certain objective criteria (in this regard, please see our response to Question 39 below) or by expressly amending the meaning of performing specified activities by way of business which clearly carves out DeFi protocols and their developers; ○ as discussed in the main body of this response letter, web3 companies are able to distribute cryptoassets associated with their protocols for free (or on a <i>de minimis</i> basis) or in connection with incentive-based rewards (for activities such as liquidity mining, staking, validation, mining, or other services), in order to allow them to decentralise their protocols, without being precluded by inappropriate or unachievable regulatory obligations. For instance, issuers of securities today benefit from exclusions from relevant specified activities – such as dealing as principal – in relation to the issue of their own shares or debentures. So excluding cryptoasset issuances from regulatory requirements when conducting free or <i>de minimis</i> consideration distributions seems uncontroversial and would provide helpful regulatory certainty to allow web3 builders to confidently operate in the UK; ○ as discussed in the main body of this response letter, cryptoassets distributed for free pursuant to the above are able to be traded on secondary markets without undue restriction and that the formation of such secondary markets is not precluded by inappropriate or unachievable regulatory obligations (keeping in mind that secondary market participants must still be protected from persons that are reasonably likely to possess significant asymmetric information about the underlying value of a cryptoasset); and ○ providers of technology services in relation to web3 ecosystems (such as mining and validation services) are not subject to the same regulation as cryptoasset intermediaries just because they provide these services. ● We also strongly recommend that cryptoassets distributed for free (or on a <i>de minimis</i> basis) or in connection with incentive-based rewards (for activities such as liquidity mining, staking, validation, mining, or other services) in relation to a decentralised protocol are not subject to the same disclosure requirements that would apply to public offers or listings of cryptoassets as part of an ICO or cryptoasset sale. The same should apply to |

| | | |
|----------|---|--|
| | | <p>any decentralised cryptoassets. As discussed in the main body of this response letter, seeking to apply traditional issuer-centric disclosure requirements in relation to such cryptoassets would be inappropriate because the same risks with respect to investor protection do not arise in relation to the issue of such cryptoassets. If disclosure requirements were to apply to such cryptoassets, as a bare minimum they should be narrowly tailored and be capable of being satisfied by on-chain data. It is critical that any such disclosures be capable of being automated, otherwise the regulatory framework could effectively enforce an element of centralisation by requiring a centralised actor to be responsible for complying / procuring compliance with disclosure requirements. Any issuer-based disclosure regime applicable to centralised cryptoassets should sunset when the protocol's cryptoassets become truly decentralised.</p> |
| <p>2</p> | <p>Do you agree with HM Treasury's proposal to leave cryptoassets outside of the definition of a "financial instrument"? If not, then please specify why.</p> | <ul style="list-style-type: none"> ● We strongly agree. Cryptoassets that do not involve rights and obligations equivalent to the kinds of investments currently captured by the definition of a financial instrument should not be included within the definition. ● We support the Treasury's view that it would be inappropriate to retrofit an existing regime to a new asset class with unique features and risks, as well as many non-financial use cases, and that for those cryptoasset activities that present similar risks to financial instruments (e.g. market manipulation practices which arise from the fact that cryptoassets are traded in a way that resembles financial instruments) it would be more appropriate to put in place a regime that provides equivalent or similar safeguards, but tailored to reflect the particularities of the relevant cryptoassets / circumstances surrounding their issue and trading. |
| <p>4</p> | <p>How can the administrative burdens of FSMA authorisation be mitigated for firms which are already MLR-registered and seeking to undertake regulated activities? Where is further clarity required, and what support should be available from UK authorities?</p> | <ul style="list-style-type: none"> ● There are some practical steps we believe could be beneficial for such firms. For example: <ul style="list-style-type: none"> ○ the introduction of a streamlined authorisations process for such firms, including that they should not be required to resubmit information already submitted to the FCA for the purposes of becoming registered under the MLRs where it has not materially changed; ○ more transparency with respect to the authorisations process overall; ○ more precise publicly available advance information about the specific information required for an application; ○ clear timeframes for processing applications post-submission which are not reliant on regulator discretion; and ○ better, more consistent, and transparent communication with authorisations case officers. |
| <p>6</p> | <p>Does the phased approach that the UK is proposing create any potential challenges for market participants? If so, then please explain why.</p> | <ul style="list-style-type: none"> ● As indicated in the main body of this response letter, we support the introduction of well-considered regulation and the phased approach proposed by the Treasury allows for this, particularly in relation to DeFi. However, as discussed elsewhere in this response letter, it will be critical that certain elements of the new cryptoasset regulatory regime that is currently proposed are appropriately limited or subject to specific express exclusions that ensure the regime does not inadvertently hamper the development of a burgeoning web3 and crypto ecosystem in the UK by imposing inapposite regulatory burdens on decentralised ecosystems now, or introducing regulatory uncertainty for web3 builders who may look to |

| | | |
|------------------|--|---|
| | | <p>establish themselves in the UK prior to a bespoke DeFi regulatory regime being established.</p> |
| <p>8</p> | <p>Do you agree with the list of economic activities the government is proposing to bring within the regulatory perimeter?</p> | <ul style="list-style-type: none"> ● In general, the activities the Treasury is proposing to regulate seem apt to capture the activities of centralised intermediaries in relation to cryptoassets, rather than decentralised protocols or software businesses. ● However, as discussed in the main body of this response letter, it will be critical to ensure that the regulatory framework that is introduced now is not overly inclusive in a way that would undermine the Treasury’s approach of seeking to further its understanding of how DeFi works before introducing a regulatory framework for it. ● As discussed in our response to Question 1 above, this could be achieved by ensuring that the activities captured by the new regime are appropriately limited in scope, or that specific express exclusions from relevant activities are included, including with respect to issuances of cryptoassets for free / <i>de minimis</i> considerations as part of a plan of decentralisation. ● In this regard, in addition to those potential exclusions suggested in our response to Question 1 above, we would also expect that exclusions from various activities equivalent to those that exist today relating to activities conducted by persons for their own account / not as a service (such as the exclusion for absence of holding out) are included in the new regulatory framework, so as to ensure that intermediaries providing services in relation to cryptoassets are not treated in the same way as market participants conducting activities on a proprietary basis (proprietary investment activity and trading in cryptoassets should not, for example, be subject to regulation). ● However, we strongly disagree with the potential inclusion of the validation and governance activities within the regulatory perimeter (even in a future phase of crypto regulation). These activities are not only essential to the concept of decentralised functionality, but they are activities that do not give rise to the same risks as the other kinds of activities the Treasury is proposing to regulate, and should remain unregulated technology services. We elaborate on the reasons for this in our response to Question 44 below. |
| <p>9</p> | <p>Do you agree with the prioritisation of cryptoasset activities for regulation in phase 2 and future phases?</p> | <ul style="list-style-type: none"> ● The suggested phasing set out in the consultation seems broadly appropriate. |
| <p>10</p> | <p>Do you agree with the assessment of the challenges and risks associated with vertically integrated business models? Should any additional challenges be considered?</p> | <ul style="list-style-type: none"> ● We agree with the Treasury’s assessment insofar as it relates to CeFi. Vertical integration within centralised businesses exacerbates the risk of unacceptable conflicts of interests and the potential for fraud, financial mismanagement, or incompetence by a small number of executives to have a disproportionately large effect on consumers and overall market stability. Accordingly, it is appropriate to consider whether such business models require additional or different regulation, similar to that which applies to equivalent or similar business models in traditional finance. We think the application of the historical lessons learned in traditional finance to such business models would likely be helpful from a consumer protection perspective and would overall add credibility to the crypto sector. However, for the reasons discussed in the main body of this response letter, we do not think the same risks arise in DeFi. |

12 Do you agree that so-called algorithmic stablecoins and crypto backed tokens should be regulated in the same way as unbacked cryptoassets?

- We agree with the Treasury’s proposal not to ban algorithmic stablecoins, however we disagree that all algorithmic stablecoins are under-collateralised and pose the same risks.
- Generally speaking, stablecoins do not fail as a result of the use of an algorithm, but rather due to collateral design.
- Under-collateralised algorithmic stablecoins are the most risky, given that the relevant 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 collapse.
- However, over-collateralised algorithmic stablecoins exist and do not pose the same risks as under-collateralised stablecoins. By ensuring that the protocol always maintains more than \$1 of collateral for every \$1 of outstanding stablecoin, stablecoin holders should always be able to redeem their stablecoins for \$1 of collateral, provided that the stablecoin is supported by exogenous capital, as explained below.
- The type or quality of collateral supporting an algorithmic stablecoin is also highly relevant to its risk profile. For these purposes, collateral can fall into two categories: endogenous collateral and exogenous collateral.
- 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 utilising 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 stablecoin 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-collateralised and backed by exogenous collateral (e.g. DAI). On the other hand, the algorithmic stablecoins that de-pegged significantly or that failed were under-collateralised stablecoins backed almost entirely by endogenous collateral (e.g., UST). For the stablecoins that have depegged

| | | |
|-----------|---|---|
| | | <p>or failed, the primary reasons have been their collateral designs, not their algorithms.</p> <ul style="list-style-type: none"> As a result of the foregoing, well-tailored stablecoin regulation should take  <p>into account the quality of the collateral being utilised to support the price of the stablecoin. Rather than treating all algorithmic stablecoins the same, regulation could permit the use of over-collateralised stablecoins backed solely by exogenous collateral with significant market caps (such as BTC and ETH), and treat these differently to under-collateralised stablecoins / stablecoins backed by endogenous capital.</p> <ul style="list-style-type: none"> We would encourage the Treasury to consider studying these differences in algorithmic stablecoin design further in determining how algorithmic stablecoins should be treated under the new UK crypto regulatory regime. |
| <p>14</p> | <p>Do you agree with the proposed regulatory trigger points - admission (or seeking admission) of a cryptoasset to a UK cryptoasset trading venue or making a public offer of cryptoassets?</p> | <ul style="list-style-type: none"> In general, we agree with the Treasury’s proposed regulatory outcomes for cryptoasset issuance and disclosures to the extent they are appropriately calibrated. However, it is imperative that the regime is tailored according to: (i) the attributes of the specific cryptoassets being offered or listed (since not all types of cryptoassets present the same risks); and (ii) the circumstances surrounding their issuance / listing. As discussed in the main body of this response letter, the risks associated with centralised cryptoassets and decentralised cryptoassets are very different and should be accounted for appropriately. |
| <p>15</p> | <p>Do you agree with the proposal for trading venues to be responsible for defining the detailed content requirements for admission and disclosure documents, as well as performing due diligence on the entity admitting the cryptoasset? If not, then what alternative would you suggest?</p> | <ul style="list-style-type: none"> Furthermore, as discussed in the main body of this response letter, we strongly feel that cryptoassets distributed for free / <i>de minimis</i> consideration or in connection with incentive-based rewards (for activities such as liquidity mining, staking, validation, mining, or other services) in relation to a decentralised protocol should not be subject to the same disclosure requirements that would apply to public offers or listings of cryptoassets as part of an ICO or cryptoasset sale. As discussed in our response to Question 1 above, seeking to apply traditional issuer-centric disclosure requirements in relation to such cryptoassets would thwart efforts to pursue full decentralisation and also be inappropriate because the same risks with respect to investor protection do not arise in relation to the issue of such cryptoassets. If disclosure requirements were to apply to such cryptoassets, |
| <p>16</p> | <p>Do you agree with the options HM Treasury is considering for liability of admission disclosure documents?</p> | |

| | | |
|----|--|--|
| 17 | Do you agree with the proposed necessary information test for cryptoasset admission disclosure documents? | <p>such as in relation to an offering of such cryptoassets by a centralised third party offeror (that did not benefit from an exemption), then, as a bare minimum they would need to be either narrowly tailored such that they could be satisfied by on-chain data, or be sunset when the protocol becomes truly became decentralised (by reference to an objective test for decentralisation).</p> <ul style="list-style-type: none"> • We support the Treasury’s proposal to introduce exemptions from the proposed issuance and disclosure regime for cryptoassets that will broadly match those that currently exist in relation to public offer requirements relating transferable securities, including for offers below a <i>de minimis</i> monetary threshold or to qualified investors only. • Generally, we agree that in relation to CeFi a sensible starting point for these regimes are the equivalent traditional finance regulatory regimes, with some scope for tailoring by the FCA, on the basis that CeFi poses many of the same risks as traditional finance, but provided that their liability for listing decentralised cryptoassets is appropriately scoped to only require publicly available information and / or on-chain data. |
| 18 | Do you consider that the intended reform of the prospectus regime in the Public Offers and Admission to Trading Regime would be sufficient and capable of accommodating public offers of cryptoassets? | |
| 19 | Do you agree with the proposal to use existing RAO activities covering the operation of trading venues (including the operation of an MTF) as a basis for the cryptoasset trading venue regime? | |
| 20 | Do you have views on the key elements of the proposed cryptoassets trading regime including prudential, conduct, operational resilience and reporting requirements? | |
| 21 | Do you agree with HM Treasury's proposed approach to use the MiFID derived rules applying to existing regulated activities as the basis of a regime for cryptoasset intermediation activities? | |
| 22 | Do you have views on the key elements of the proposed cryptoassets market intermediation regime, including prudential, conduct, operational resilience and reporting requirements? | |
| 23 | Do you agree with HM Treasury’s proposal to apply and adapt existing frameworks for traditional finance custodians under Article 40 of the RAO for cryptoasset custody activities? | |
| 24 | Do you have views on the key elements of the proposed cryptoassets custody regime, including prudential, conduct and operational resilience requirements? | |
| | | |

| | | |
|----|---|---|
| 25 | Do you agree with the assessment of the challenges of applying a market abuse regime to cryptoassets? Should any additional challenges be considered? | <ul style="list-style-type: none"> • We are in favour of market abuse regulation applying to cryptoassets, with the caveat being that these rules must be specially tailored for decentralised issuers and DeFi, including in order to enable decentralised exchange protocols to exist. |
| 26 | Do you agree that the scope of the market abuse regime should be cryptoassets that are requested to be admitted to trading on a cryptoasset trading venue (regardless of where the trading activity takes place)? | |
| 27 | Do you agree that the prohibitions against market abuse should be broadly similar to those in MAR? Are there any abusive practices unique to cryptoassets that would not be captured by the offences in MAR? | |
| 28 | Does the proposed approach place an appropriate and proportionate level of responsibility on trading venues in addressing abusive behaviour? | |
| 29 | What steps can be taken to encourage the development of RegTech to prevent, detect and disrupt market abuse? | |
| 30 | Do you agree with the proposal to require all regulated firms undertaking cryptoasset activities to have obligations to manage inside information? | |
| 31 | Do you agree with the assessment of the regulatory challenges posed by cryptoasset lending and borrowing activities? Are there any additional challenges HM Treasury should consider? | <ul style="list-style-type: none"> • We are in favour of regulations applying to cryptoasset lending, with the caveat being that these rules must be tailored to enable DeFi to exist. |
| 32 | What types of regulatory safeguards would have been most effective in preventing the collapse of Celsius and other cryptoasset lending platforms earlier this year? | |
| 33 | Do you agree with the idea of drawing on requirements from different traditional lending regimes for regulating cryptoasset | |

| | | |
|-----------|---|---|
| | <p>lending? If so, then which regimes do you think would be most appropriate and, if not, then which alternative approach would you prefer to see?</p> | |
| <p>34</p> | <p>Do you agree with the option we are considering for providing more transparency on risk present in collateralised lending transactions?</p> | |
| <p>35</p> | <p>Should regulatory treatment differentiate between lending (where title of the asset is transferred) vs staking or supplying liquidity (where title of the asset is not transferred)?</p> | <ul style="list-style-type: none"> ● Yes. Lending and staking are distinct activities which serve entirely different purposes in relation to web3 and crypto. ● On the one hand, staking is a mechanism which is used by many web3 protocols as a means of ensuring the security of the protocol and incentivising actions necessary for the protocol to function. For example, “proof of stake” protocols will often require that in order to interact with the protocol in certain ways / perform certain actions (such as transaction validation), an amount of cryptoassets must first be staked by the relevant person. This creates a natural and powerful disincentive for such persons to engage in malicious activity in relation to the protocol because they have “skin in the game” by virtue of the cryptoassets they have staked. Typically, provided the relevant person does not act in a way contrary to the objective required standards of the relevant protocol (in which case their cryptoassets may be at risk of “slashing”), a person is not at risk of losing their cryptoassets as a result of staking them and does not surrender control of them to a third party in order to stake them. Rewards are often also distributed to stakers on their staked cryptoassets as a means of incentivising third parties to perform actions necessary for the functioning of the protocol (the latter being essential for decentralisation, like transaction validation). ● On the other hand, lending is principally used as a means of facilitating the rehypothecation of cryptoassets, either by a centralised business with a view to generating profits or income from its reuse of borrowed cryptoassets or in decentralised exchanges to facilitate the exchange of cryptoassets by users of the exchange. Lending therefore involves a transfer of cryptoassets by one person to another, in exchange for a contractual promise for their return at a future time or, in the case of a decentralised exchange, a technological ability to effect their return from the protocol. ● As is clear from the principal differences between lending and staking, they do not give rise to the same risks and so do not warrant the same regulation. In particular, staking does not give rise to counter-party risk, as it does not involve the transfer of control over cryptoassets, meaning that a staker, unlike a lender of cryptoassets, does not require protection from the potential misfeasance or incompetence of a centralised business operating a cryptoasset lending scheme, or the malfunction of a protocol into which they have deposited their assets for reuse. ● Important policy considerations must also be considered. For example, any particular jurisdiction’s decision to regulate staking is likely to represent the imposition of a prohibitively expensive and anti-competitive regulatory burden on web3 startups, given the widespread use of staking by web3 protocols that employ proof of stake mechanisms to secure the protocol and incentivise third parties to perform actions necessary for the functioning of |

| | | |
|------------------|--|--|
| | | <p>the protocol (the latter being essential for decentralisation, as discussed in the main body of this response letter). Accordingly, this is a topic in relation to which the policy objective of encouraging growth and innovation seems likely to outweigh others (particularly given the discussion above about staking presenting a lower risk from an investor protection perspective than lending). Regulation of staking may also risk web3 protocols favouring other, less environmentally friendly mechanisms, such as “proof of work” mechanisms, if staking is regulated but they are not.</p> |
| <p>36</p> | <p>Do you agree with the assessment of the challenges of regulating DeFi? Are there any additional challenges HM Treasury should consider?</p> | <ul style="list-style-type: none"> ● Please see our comments in the main body of this response letter, and our responses to the various other specific Consultation questions. |
| <p>38</p> | <p>Do you agree with HM Treasury's overall approach in seeking the same regulatory outcomes across comparable "DeFi" and "CeFi" activities, but likely through a different set of regulatory tools, and different timelines?</p> | <ul style="list-style-type: none"> ● Please see our comments in the main body of this response letter, and our responses to the various other specific Consultation questions. |
| <p>39</p> | <p>What indicators should be used to measure and verify “decentralisation” (e.g. the degree of decentralisation of the underlying technology or governance of a DeFi protocol)?</p> | <ul style="list-style-type: none"> ● As set forth in the body of this letter, in the context of assessing the decentralisation of a cryptoasset, it is our view that it is likely necessary for regulators to use a principles-based approach, and it is worth further exploring objective criteria that can be established. ● As set forth in the body of this letter, in the context of assessing the decentralisation of a blockchain or smart contract protocol for regulatory purposes, it is our view that it is critical that decentralisation be capable of being assessed objectively by reference to statutory criteria, rather than being dependent on regulatory discretion in each case. As a minimum, we would recommend that the following criteria should be met by a protocol in order for it to be considered decentralised for regulatory purposes: <ul style="list-style-type: none"> ○ information regarding its operation is transparent and available to all (enabled by transparent blockchain ledgers); ○ the protocol is composed of source code that is publicly available and accessible and whose primary purpose cannot be materially altered or disabled by a single person or group of persons acting pursuant to an express or implied agreement, and is designed to prevent any such person or persons from amending or reversing transactions executed and recorded on the blockchain; and ○ public participants have the ability to execute digital asset transactions through such protocol in accordance with predetermined non-discretionary automated rules or algorithms. ● In the main body of this response letter, we refer to a blockchain or smart contract protocol that meets these criteria as “fully-functional”. These criteria could therefore usefully be deployed in a regulatory regime to define decentralised protocols and to establish relevant exclusions / derogations from certain regulatory requirements for such protocols (or certain actors in relation to them) where appropriate. ● Notably, the concept of a decentralised protocol being “fully-functional” is distinct from what might be thought of as “true” decentralisation, which may |

| | | |
|-----------|---|--|
| | | <p>demand a more subjective assessment of the facts and circumstances relating to a particular blockchain or smart contract protocol that may change over time. Indeed, it is for this reason that we suggest the “fully-functional” criteria are the most apt to define what is a decentralised network / protocol for regulatory purposes, since they are more capable of objective determination, their satisfaction (or otherwise) is less likely to fluctuate over time, and, crucially, they allow for a regulatory approach which recognises that decentralisation is a process that decentralised protocols (and their developers) must undergo (likely from a centralised (or at least not a “truly” decentralised) starting point.</p> |
| <p>40</p> | <p>Which parts of the DeFi value chain are most suitable for establishing "regulatory hooks" (in addition to those already surfaced through the FCA-hosted cryptoasset sprint in May 2022)?</p> | <ul style="list-style-type: none"> ● As per our comments in the main body of this response letter, we strongly believe that businesses providing apps that facilitate access to or the use of protocols, and not the protocols themselves (nor the developers of such protocols), are the appropriate hook for regulatory obligations in relation to web3, including DeFi. ● Regulation of such apps as the “gateways” to the DeFi ecosystem should be sufficient to achieve the main legitimate policy objectives of investor protection and curtailment of illicit market activity that typically drive the need for regulation. ● However, even then, it will ultimately not be necessary or appropriate to regulate all such apps in the same way. To give a specific example, the policy objectives underlying AML / CTF can be accomplished without applying know your customer requirements to DeFi applications or protocols. Although AML / CTF requirements aid authorities in the investigation of illegal conduct, investigators have been able to effectively obtain required evidence in practice from fiat on- and off-ramps that are already covered by AML / CTF obligations, such as centralised exchanges, payment processors, and banks. For example, the existing regulatory controls already applicable to money transmitters, including centralised exchanges (e.g. Coinbase and Gemini) and other virtual asset service providers (e.g. Transak and Moonpay), require them to verify the identities of users bringing funds on-chain. This information allows investigators in the private sector, law enforcement, and regulatory communities to collect attribution information of users conducting transactions via these mechanisms, including any transaction executed via a decentralised exchange. ● Indeed, this logic appears to have already been accepted by policy makers with respect to the introduction of the so-called “travel rule” in relation to crypto, which will generally only require money transmitters and virtual asset service providers to gather and send relevant information, and not other businesses who may interact with unhosted wallets. ● The general principle that not all apps should be regulated in the same way is also evident in the current UK regulatory framework applicable to cryptoassets and payment services, which, for example, do not capture technology service providers who provide services adjacent to regulated activities (such as payment gateway providers or non-custodial wallet providers).²⁸ |

²⁸ See Joint Money Laundering Steering Group, *Guidance For The UK Financial Sector Part II: Sectoral Guidance*, at 22.12, 22.16, 22.25 and 22.26 (Jun. 2020 amended Jul. 2022), https://www.jmlsg.org.uk/wp-content/uploads/2022/09/JMLSG-Part-II_July-2022.pdf; see also the exclusion for technical service providers

| <p>41</p> | <p>What other approaches could be used to establish a regulatory framework for DeFi, beyond those referenced in this paper?</p> | <ul style="list-style-type: none"> • The characteristics of a given web3 app establish what risks such app may create and therefore play a significant role in determining whether and to what extent regulation should apply. Such characteristics reveal where asymmetric information risk, centralisation risk, or market integrity risk from size and impact over the trading environment could exist. • For example, many web3 apps may not be entirely trustless, for instance, because they take custody of user assets, intermediate user’s transactions, and / or market or advertise certain assets, products, or services to users. Apps with these characteristics are the most likely to require regulation since they are more likely to introduce legacy centralisation risks to users or, if left unregulated, to run counter to policy objectives. • Beyond characteristics that introduce centralisation risks, two important characteristics of web3 apps also have regulatory implications where web3 technology doesn’t obviate a regulation’s purpose. These are (i) whether the app is operated by a business for profit and (ii) whether the app’s intended primary purpose is to facilitate an otherwise regulated activity. Although it is possible to analyse many additional characteristics and how they affect the risk profile of a given app, these two factors are obvious jumping off points which can usefully be taken into account when seeking to balance policy objectives in DeFi regulation. • For example, these characteristics may indicate where the desire to foster innovation may outweigh the need for regulation, as it may be appropriate that non-profit apps are regulated differently to for-profit apps, or that general purpose block explorer apps are simply software and need no regulation. • The following image summarises the approach described above: <div data-bbox="646 1193 1544 1686" data-label="Figure"> <p>SAME USER ACTIVITIES, DIFFERENT USER RISKS, DIFFERENT RULES</p> <table border="1"> <caption>Risk Profile and User Experience by App Type</caption> <thead> <tr> <th>App Type</th> <th>Risk Profile (High to Low)</th> <th>User Experience (Least to Most)</th> </tr> </thead> <tbody> <tr> <td>Centralized Exchange (CEX)</td> <td>High (Custodial risks, Conflicts of interest risk, Risk arising from access to certain assets)</td> <td>Least web3 experience</td> </tr> <tr> <td>For-Profit Decentralized Exchange (DEX) App</td> <td>Medium-High</td> <td>Low</td> </tr> <tr> <td>Nascent For-Profit DEX App</td> <td>Medium</td> <td>Low-Medium</td> </tr> <tr> <td>Not For-Profit DEX App</td> <td>Medium-Low</td> <td>Medium</td> </tr> <tr> <td>Block Explorer App</td> <td>Low</td> <td>Most web3 experience</td> </tr> </tbody> </table> <p>Need for regulation outweighs supporting innovation (for CEX)</p> <p>Supporting innovation outweighs need for regulation (for Block Explorer App)</p> </div> | App Type | Risk Profile (High to Low) | User Experience (Least to Most) | Centralized Exchange (CEX) | High (Custodial risks, Conflicts of interest risk, Risk arising from access to certain assets) | Least web3 experience | For-Profit Decentralized Exchange (DEX) App | Medium-High | Low | Nascent For-Profit DEX App | Medium | Low-Medium | Not For-Profit DEX App | Medium-Low | Medium | Block Explorer App | Low | Most web3 experience |
|---|---|--|----------|----------------------------|---------------------------------|----------------------------|--|-----------------------|---|-------------|-----|----------------------------|--------|------------|------------------------|------------|--------|--------------------|-----|----------------------|
| App Type | Risk Profile (High to Low) | User Experience (Least to Most) | | | | | | | | | | | | | | | | | | |
| Centralized Exchange (CEX) | High (Custodial risks, Conflicts of interest risk, Risk arising from access to certain assets) | Least web3 experience | | | | | | | | | | | | | | | | | | |
| For-Profit Decentralized Exchange (DEX) App | Medium-High | Low | | | | | | | | | | | | | | | | | | |
| Nascent For-Profit DEX App | Medium | Low-Medium | | | | | | | | | | | | | | | | | | |
| Not For-Profit DEX App | Medium-Low | Medium | | | | | | | | | | | | | | | | | | |
| Block Explorer App | Low | Most web3 experience | | | | | | | | | | | | | | | | | | |
| <p>42</p> | <p>What other best practices exist today within DeFi organisations and infrastructures that should be formalised into industry standards or regulatory obligations?</p> | <ul style="list-style-type: none"> • Code audits are an important best practice that we think can be harnessed to facilitate the policy objectives of investor protection and curtailment of illicit market activity in relation to DeFi. • For example, requiring certain apps that provide access to DeFi protocols to conduct code audits in relation to the underlying protocols could protect an | | | | | | | | | | | | | | | | | | |

who do not come into possession of funds set out in paragraph 2(j) of Part 2 of Schedule 1 to the Payment Services Regulations 2017, <https://www.legislation.gov.uk/uksi/2017/752/schedule/1/part/2>.

| | | |
|------------------|--|---|
| | | <p>app’s users against smart contract failures of an underlying protocol. Code audits could also be extended to cover the app-smart contract integration to provide assurances that the app provider is not engaging in deceptive activity, such as frontrunning user trades or quoting users slightly higher prices and keeping the difference.</p> |
| <p>44</p> | <p>Is there merit in regulating mining and validation activities in the UK? What would be the main regulatory outcomes beyond sustainability objectives?</p> | <ul style="list-style-type: none"> ● We are strongly opposed to the regulation of mining and validation activities in the UK. These activities are more akin to technology services and their inclusion may risk capturing elements of the tech stack for crypto which form the baselayer required for the operation of DeFi protocols. ● Most of the same arguments made in the main body of this response letter in relation to DeFi protocols can be extended to mining and validation activities. Generally speaking, these activities do not present the same types of risks that are typically covered by financial regulations, which means it would be inappropriate to seek to regulate miners and validators in the same way as intermediaries in relation to cryptoassets. ● For example, miners and validators are generally not aware of, and are indifferent to, the nature or purpose of the underlying transactions that they work to validate. Accordingly, it would be practically impossible for miners or validators to comply with many obligations that would typically apply in relation to intermediaries (for example, requirements to monitor and report suspicious transactions). For the same reason, it would also be practically impossible for miners or validators to comply with requirements not to process certain kinds of transactions (e.g. those related to illicit activity), and attempting to impose this kind of regulation on these actors would introduce the need for miners and validators to censor transactions on the blockchain which would run contrary to one of the central tents of decentralisation that makes web3 protocols useful (per our letter above). |
| <p>45</p> | <p>Should staking (excluding “layer 1 staking”) be considered alongside cryptoasset lending as an activity to be regulated in phase 2?</p> | <ul style="list-style-type: none"> ● As discussed in our response to Question 35 above, we are strongly opposed to the regulation of staking. |
| <p>46</p> | <p>What do you think the most appropriate regulatory hooks for layer 1 staking activity would be (e.g. the staking pools or the validators themselves)?</p> | |