April 2023

Response to HM Treasury's Consultation and Call for Evidence, "Future Financial Services Regulatory Regime for Cryptoassets"

Introduction

Polygon Labs respectfully submits this response to HM Treasury's Consultation and Call for Evidence entitled "Future financial services regulatory regime for cryptoassets" (with chapters 1-10, referred to as the "Consultation" and chapters 11-13, referred to as the "Call for Evidence").[1]

Polygon Labs, an international software development company that builds blockchain infrastructure solutions and complementary software, believes that a blockchain-based Internet will enhance the ways in which we transact and interact in society. For that reason, Polygon Labs' mission is to provide more efficient and open blockchain infrastructure on which third party developers and the global community can build.

Creating a regulatory regime for "cryptoassets" that both encourages innovation and achieves the tripartite policy goals of protecting consumers, preserving market integrity, and combating illicit finance will achieve two critical missions: *first*, it will provide clarity to industry and protection for users and consumers, and *second*, it will bring the UK closer to its goal of being a "global hub for cryptoasset technology and investment".[2]

We are broadly supportive of the proposal set forth in the Consultation – HM Treasury's recognition that it should aim to achieve the "same regulatory outcome" rather than imposing the "same regulations" on this new asset class and industry will allow for robust, evergreen laws and the phasing of regulation for this industry will provide additional clarity.

Given the Consultation's focus on matters concerning centralised or custodial cryptoasset activities ("CeFi"), we expect that many responses will focus on that area of the cryptoasset ecosystem. Accordingly, Polygon Labs' response (the "Response") focuses on some narrow matters raised in the Consultation and more fully to matters in the Call for Evidence relating to *decentralised* blockchain-based technology.

[1] Capitalised terms used herein refer to defined terms used in the Consultation and Call for Evidence.

[2] https://www.gov.uk/government/news/government-sets-out-plan-to-make-uk-a-global-cryptoasset-technology-hub.

Part I. Consultation

Definition of cryptoassets and legislative approach (Chapter Two)

Question 1. Do you agree with HM Treasury's proposal to expand the list of "specified investments" to include cryptoassets? If not, then please specify why.

We agree with HM Treasury's use and definition of the term "cryptoassets"[3], but do not agree that *all* cryptoassets should be defined as "specified investments" under the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544) ("RAO"). Per the RAO, "specified investments" are various types of financial market assets that require oversight by a financial services regulator (*e.g.*, the Financial Conduct Authority ("FCA")), whereas many cryptoassets - including a number of those listed in the Consultation - do not resemble or have the characteristics of a financial market asset.

The RAO sets forth the "specified investments" over which the FCA has regulatory authority, and includes deposits, electronic money, contracts of insurance, debentures, options, futures, and stakeholder pension schemes, among others.[4]

The Consultation itself recognises various cryptoassets do not have financial or economic aspects to them and/or do not have the features of such. For example, the Consultation notes that NFTs are "cryptoassets which confer digital ownership rights of a unique asset (*e.g.*, a piece of digital art), using a technology such as DLT to support the recording or storage of data. NFTs do not provide the rights or features associated with a security token and do not function as a means of payment";[5] and "fan tokens" "give holders access to a variety of fan-related membership perks like voting on club decisions, rewards, merchandise designs and unique experiences".[6]

Thus, we respectfully request that HM Treasury take one of two narrow approaches to defining what types of cryptoassets are classified as "specified investments". *First*, HM Treasury could include specific definitions of the types of cryptoassets which constitute "specified investments", leveraging the "Glossary of commonly used terms for cryptoassets" in the Consultation to include only those cryptoassets that have features similar to the assets and instruments already defined in the RAO's list of "specified investments". *Second*, HM Treasury could have a section on "exclusions" from "specified investment" to eliminate those cryptoassets that do not have characteristics of or uses as financial or economic assets. We understand that the second approach may be preferable given its consistency with the RAO's definition and the FCA Handbook on "specified investments".[7]

---

[3] The term "cryptoasset" is more precise and technologically correct than the term "digital asset" because many assets are "digitised", including both financial instruments as well as expressly non-financial instruments (*e.g.*, airline rewards miles).

[4] Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (SI 2001/544), Part III. See also https://www.handbook.fca.org.uk/handbook/glossary/G1117.html.

[5] The Consultation clearly states that NFTS "will not be in scope of the cryptoassets financial promotions regime", but a more explicit exclusion from the definition of "specified investments" – along with other similarly varied cryptoassets – is important to achieve regulatory clarity.

[6] Consultation, Box 2.A.

[7] *See, e.g.*,FCA Handbook, *available at* https://www.handbook.fca.org.uk/handbook/PERG/2/6.html, PERG 2.6.3 (noting the transactions excluded from the definition of "deposit" classified as a "specified investment").

Question 2. 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.

We agree with HM Treasury's proposal to exclude "cryptoassets" from the definition of "financial instrument".

Cryptoasset Activities (Chapter Four)

Chapter Four of the Consultation addressing various "cryptoasset activities" necessarily undertakes an analysis of the various types of "cryptoassets" and recognises that "cryptoassets" is a broad term, encompassing a wide range of uses and deployments, some financial and some divorced entirely from any economic use or benefit. This nuanced approach, particularly the Glossary available in Box 2A of the Consultation, provides enhanced clarity even at this early stage.

The one term that is used throughout the Consultation but is not defined is "unbacked cryptoassets". We understand this term to mean any cryptoasset that does not have any other asset or item to which its value is tied, given the Consultation's reference to "Bitcoin" as an "unbacked cryptoasset".[8] The industry would benefit from a precise definition of "unbacked cryptoasset" in order to distinguish it from other types of cryptoassets that may exist or be developed that could be classified as not having "backing" or "sufficient backing".

Further, the Consultation does not engage in a specific discussion of how HM Treasury intends to "regulate" "unbacked cryptoassets" but it does specify that "the government intends to regulate financial services ***activities***, rather than the assets themselves", which provides clarity that only when an "unbacked cryptoasset" is involved in a "regulated activity" will it fall under regulatory purview via the regulated *individual* or *entity*, not as an asset standing alone.[9]

As it relates to "unbacked cryptoassets", some cryptoassets (*e.g.*, Bitcoin and Ether) do not have their value "tied" to any other asset that exists outside a blockchain or otherwise, because their primary purpose is to power and secure a blockchain network; this is an intended feature of the technology. In other cases, a cryptoasset may be unbacked but may enable some other benefits for users (*e.g.*, discounts, exclusive access, etc.) while not serving an inherent blockchain purpose. This is akin to the definition of "fan token" in the Consultation's Glossary of cryptoassets.

Ultimately, cryptoassets that have no specific backing but are a part of the underlying technology are fundamentally different from cryptoassets that have no backing and should be treated differently. This would be consistent with the principle of regulating cryptoasset *activity* rather than regulating cryptoassets *themselves*.

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

HM Treasury proposes to "regulate" algorithmic stablecoins and "cryptobacked tokens" through the "cryptoasset financial promotion rules" by restricting centralised actors who engage in

[8] Consultation, § 4.21.

[9] Consultation, § 4.13.

activities with such cryptoassets from marketing them as "stable", "payment instruments" or using "very similar terms where the use of those terms would be misleading".[10]

We agree that the most appropriate way to regulate "unbacked cryptoassets", "algorithmic stablecoins" or "cryptobacked tokens" is to (a) elucidate precisely what ***activities*** involving those cryptoassets require registration or fall under regulatory purview; and (b) set forth clear disclosure rules on a registrant that mandate precise and full information about the way in which such cryptoassets work from a technological perspective and any attendant risks arising from those cryptoassets, and require accurate marketing by the relevant registrant relating to such cryptoassets.

Question 13. Is the proposed treatment of NFTs and utility tokens clear? If not please explain where further guidance would be helpful.

The Consultation specifies that NFT's and utility tokens will only fall under the UK's financial regulation for cryptoasset activity if they are used in specified financial activity – *e.g.*, issuance activity such as admitting a cryptoasset to a cryptoasset trading venue; payment activities or lending or borrowing activities, among others.[11]

Although this may be technically correct, it overlooks that activities relating to NFTs do fall under some of the proposed regulated cryptoasset activities. For example, artists may "issue" NFTs – individually or as part of a series; trading venues may allow users to trade NFTs – either for other NFTs or for crypto or fiat currency; and other entities or protocols may allow users to lend NFTs or portions thereof in exchange for other NFTs or other cryptoassets. Some of this activity may fall under certain types of proposed regulated financial activity; while other activity – even if it has an economic component (*e.g.*, sale of art) – will expressly not fall under this type of regulated activity since it has clear non-regulated corollaries in the analog world (*e.g.*, auctions for art). Further stakeholder engagement and a call for evidence may be helpful in clarifying the scope and usage of NFTs for various activities to determine whether and how such activities should fall under the proposed scope of regulated financial activity.

As it relates to utility tokens, which the Consultation defines as "cryptoassets which provide digital access to a specific service or application . . . and use a technology such as DLT to support the recording or storage of data" and constitute "unbacked cryptoassets", we encourage HM Treasury to consider expressly stating that cryptoassets used for paying gas fees as a subset of utility tokens. This recognition is critical because these cryptoassets enable validators to secure the network and do not involve the type of regulated financial activity as proposed in the Consultation.

In addition, we respectfully suggest that HM Treasury consider how to treat cryptoassets that may fall into more than one category. Particularly, should these cryptoassets receive a new classification or should they fall under a "predominant" classification.

[10] Consultation, §§ 4.21, 4.25.

[11] Consultation, § 4.28 & Table 4.A.

Part II. Call for Evidence

Decentralised Finance (Chapter Eleven)

Decentralised finance or "DeFi" is a software system that enables users to engage in economic transactions and activities in a self-directed manner without the need for or use of traditional financial intermediaries.

We agree with HM Treasury's statement that "DeFi presents complex and unique challenges for policy makers and regulators". This is consistent with the statement from the International Monetary Fund ("IMF") that "DeFi calls for creative risk mitigation" in any regulatory response.[12] For this reason, it will take "longer to clarify" how or whether to regulate DeFi and thus, such proposals for DeFi should fall into the later stages of HM Treasury's comprehensive approach to regulation in the cryptoasset sector. The most critical challenge in "regulating DeFi" is to ensure that any regulation does *not* force centralisation into the system where it otherwise does not exist. The discussion below presents the Call for Evidence with this in mind.

Question 36. Do you agree with the assessment of the challenges of regulating DeFi? Are there any additional challenges HM Treasury should consider?

As set out in the Call for Evidence, the greatest "challenges" in "regulating DeFi" emanate from questions about "decentralisation" – namely, determining the level of decentralisation in "governance mechanisms" and the global and borderless nature of DeFi, "with participants operating across many jurisdictions" such that "typical systems of financial services regulation – which usually rely on the authorisation and supervision of individuals and firms undertaking specified activities - may be difficult to apply".[13]

Regulatory goals, including protecting consumers, preserving market integrity, and combating illicit finance can be met in the DeFi ecosystem, but achieving such goals will require different regulatory tools and mechanisms than in the traditional finance system. Novel compliance solutions seek to achieve the same regulatory outcomes in DeFi systems through technological advancements.

Question 37. How can the size of the "UK market" for DeFi be evaluated? How many UK-based individuals in DeFi protocols? What is the approximate total value locked from UK-based individuals?

When referring to truly decentralised systems, it is impossible to determine a UK-nexus "for DeFi", including the number of UK users accessing DeFi protocols, or the value or amount of cryptoassets UK-based individuals supply to DeFi protocols because the location of users cannot be determined on blockchains.

DeFi protocols are software deployed to a permissionless blockchain network (most frequently, Ethereum). Blockchain networks run through "nodes" (*i.e.*, computers operated by hundreds or thousands of persons), which validate transactions. In most decentralised systems, nodes are located around the world with little indication regarding exact location. For this reason,

[12] IMF Policy Paper, "Elements of Effective Policies for Cryptoasstes", ¶ 59.

[13] Consultation, § 11.2.

blockchain networks – and the software deployed upon them – are, as the Call for Evidence notes, borderless and global; therefore, DeFi protocols are not "based" in any single location.

In addition, truly decentralised DeFi protocols can be accessed primarily through self-hosted wallets – which are pseudonymous and do not provide what is typically thought of as "personally identifiable information" (*e.g.*, name, email, IP address, etc.). "Front end interfaces" (also called "user interfaces" or "front ends") that simplify access to DeFi protocols using those wallets do not necessarily collect information relating to IP addresses (another way to identify the location of a user); further, some front ends are hosted via decentralised systems for hosting and sharing data (*e.g.*, the Interplanetary File System ("IPFS")), which do not allow for collecting IP addresses. In many instances, there are dozens of front ends or other access points to DeFi protocols making it virtually impossible to track and obtain users' identities, IP addresses, or locations. Furthermore, users can access DeFi protocols directly on a blockchain network, without the use of any front end or a centralised access point, making it impossible to know their locations.

Given the decentralised nature of DeFi protocols as well as the way in which users interact with these protocols, it is impossible to know the size of the "UK market" for DeFi, how many UK-based individuals use DeFi protocols, or the "total value" of cryptoassets supplied from UK-based individuals. This information is equally unknown for all other jurisdictions and their respective DeFi markets.

A UK "market" size for DeFi may be evaluated via future centralised registrants, who already are or may eventually come under the FCA's jurisdiction, who are located in the UK and who may provide access to DeFi protocols to UK users, albeit that data would represent a lower bound and fraction of the market size.

Question 38. 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.

We agree that "same regulatory outcome" is a sensible approach to regulating novel financial activity that has arisen with innovation that disintermediates or fundamentally changes how functions are performed.

We further agree with HM Treasury's claim that different cryptoasset activities present different forms of risk and that there is no "one size fits all" approach to regulation. This is particularly true because the *source* of risk in DeFi systems is significantly different than that in centralised systems, like CeFi or the traditional financial system. To this end, it may be more accurate to update: "same risk, same regulatory outcome" to "*different source* of risk, same regulatory outcome".

In fully decentralised systems, risk to users and to market integrity is borne primarily from technology and cyber risks, or the risks of integration with centralised systems (*e.g.*, centrally issued tokens or centralised information systems such as oracles), whereas in traditional financial systems, risk is borne primarily from concentration of data or information or errors in human or subjective judgment. In this Response, "technology risk" refers to code being inherently unsafe for use due to code errors and bugs and "cyber risk" refers to instances where the protocol is

functioning and being used as intended but a "loophole" may exist – and/or may not have been detected during security audits of the code – that allows an individual to exploit the code to gain an unfair advantage.

In the traditional financial system, Person A, the user, could lose assets due to the misuse of those assets by Person B, the individual or entity securing them. In decentralized systems, Person A could lose assets due to a bug in software. The potential risk of loss may be the same, but the regulation applied to those systems should not be the same. If the decentralized system gives Person B the ability to control assets in a software system in a centralised manner, then the *source* of the risk – loss of assets – should result in the same regulation.

Various innovative compliance tools and solutions have been built and deployed – with numerous others in development – which may assist with reaching the "similar regulatory outcomes" HM Treasury seeks to achieve, bringing some parity between centralised or traditional financial systems and a more novel, innovative decentralised system.[14]

Question 39. 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)?

DeFi's innovation has led to questions about how to determine whether a DeFi protocol is "truly decentralised". Given the varying and novel aspects of blockchain-based technology, many policymakers and those in industry have found it challenging to draft a holistic, single definition. A multi-factor approach to "measur[ing] and verify[ing] 'decentralisation'" will allow for determinations on whether a DeFi protocol is "decentralised".

Various modifiers have been used with the term "decentralisation" – *e.g.*, "sufficiently", "meaningfully", etc. - in recognition that this distributed nature may be part of a "spectrum". Determinations on decentralisation should be made with the fundamental characteristics of DeFi in mind: to enhance transparency in the system and to ensure that individuals or institutions did not have to trust or rely upon an external, third party for their own financial transactions or economic well-being, including for information about those transactions.

Many have suggested that the existence of a single point of failure or control in the protocol, including any accompanying governance system, should be the determinant of decentralisation. We agree that in decentralised systems, the hallmark should be "control" – not "custody" – to determine whether there is a "regulatable" individual or entity.

The complex nature of DeFi systems necessitates a multi-factor approach to determining "decentralisation". We caution against using an overly-prescriptive definition of "decentralisation" because decentralised blockchain-based applications, including in DeFi, continue to evolve from a number of perspectives. Thus, any test must be based on tenets surrounding decentralisation: self-reliance for and independence over one's own transactions and for information about such transactions.

[14] *See* Consultation § 2.7 (recognising that HM Treasury seeks to "deliver a level playing field between crypto and traditional financial services firms conducting the same activity").

We propose a three-prong test with certain sub-factors that can be used, at least on a preliminary basis, to determine whether a DeFi protocol is "decentralised". The following factors provide a solid foundation in determining "decentralisation": technology, governance/administration, and user/ecosystem reliance.

Technology focuses on the code of the DeFi protocol: *is the code for the protocol open source or, at a minimum, source available*? Ensuring that the entire code for a DeFi protocol is open, transparent and available for anyone to view at any time demonstrates how the protocol works and allows individuals to independently verify that there are no points of centralisation in the protocol. If one views the code and is *not* able to determine how the DeFi protocol functions – or even how certain aspects of the protocol occur, then one can credibly assume that certain activities occur through a centralised individual or entity (*e.g.*, if the user cannot determine how the code of a DeFi protocol generates yield, then the user may assume that a centralised entity is creating the yield). Other factors, including the network or "chain" on which the DeFi protocol is deployed, may also assist with "measuring" technological decentralization.

Governance and administration relates to the authority over the functioning of the code, and by extension, potentially over third party user assets that are supplied to or otherwise used in the protocol: *(a) is there an administrative key that allows for control of the protocol and if so, does an identifiable natural person or entity (or group of persons who know each other and intentionally coordinate with each other) hold the key; and (b) is there a central decision-making authority that can control the protocol through governance votes or otherwise?*

One key issue that is frequently overlooked in assessing governance – even in the face of certain actors purportedly having outsized "voting influence" in distributed governance systems, such as decentralised autonomous organisations ("DAOs") – is whether users ultimately have control over their assets regardless of governance votes. Even if a DAO makes changes or updates a DeFi protocol, users should be able to (i) receive information about the changes to the protocol in a timely manner; and (ii) make decisions about removing or otherwise changing the configuration of their assets prior to such changes taking place such that any change by the DAO would not affect user assets. If users ultimately have control over their assets regardless of how a DAO (or any other form of governance) votes, then "voting power" may not be the appropriate metric for determining "control" over a DeFi protocol to affect a determination on "decentralisation".

Finally, *user/ecosystem reliance* accounts for impact, whether direct or indirect, by identifiable actors (*i.e.*, the original software or an identifiable person or group of persons coordinating with each other). This concept emanates from traditional consumer protection laws and concepts: if an identifiable party or group of persons coordinating with each other are maintaining a protocol based on representations and/or actions of that actor/group, then – even if the protocol is technologically and administratively decentralised – there still may be points of centralisation that require certain types of disclosures to ensure adequate consumer protections.

Some DeFi protocols may "meet" the above-listed factors in various ways and DeFi protocols and their attendant systems may function in varied ways; accordingly, any definition of "decentralisation" must be flexible and account for the "regulatory outcome" looking to be achieved. We do not mean to suggest that a DeFi protocol that does not meet all three of the

above prongs is automatically regulated as a centralised financial intermediary; it is possible that other regulations may apply that achieve the same "regulatory outcomes".

Question 41. What other approaches could be used to establish a regulatory framework for DeFi, beyond those referenced in this paper?

The Call for Evidence discusses the following proposed models for "regulating DeFi" (we provide commentary on each in italics in the footnotes):

- "[D]efine a set of DeFi-specific activities – *e.g.*, 'establishing or operating a protocol' - as regulated activities under the RAO (or DAR)" and then "requir[ing] authorisation" for such activities, with a "bespoke regime" from the FCA;[15]
- "[A]pply rules to persons who maintain significant control or influence over a DeFi arrangement or protocol providing cryptoasset services and activities", including but not limited to those who "maintain, run and operate systems used for regulated financial activities" (even if such persons includes the original software developer);[16]
- "Focus regulatory responsibility for mitigating risks on centralised on and off ramps like exchanges";[17] and
- Regulate "[i]nterface providers and other actors facilitating consumer access to DeFi (*e.g.*, aggregators and other consumer "front ends", by requiring them "to demonstrate or check whether certain standards or rules have been met, before facilitating access to a decentralised application or service".[18]

As an initial matter, if there is a point of centralisation in the operation of a "DeFi" protocol, whether it be operational, administrative or otherwise, then the individual or entity engaging in such conduct must consider whether they meet the type of financial services activities provided by identifiable intermediaries that is addressed in the Consultation (*e.g.*, providing a cryptoasset exchange). They would not meet the proposed test for decentralisation set forth above (or likely any other credible test for decentralisation), which is consistent with the recognition in the Call for Evidence that "Centralised business models which brand and market themselves as DeFi in

[15] Consultation § 11.5. *We believe this model is flawed because it seeks to bring those who "establish" a protocol under regulatory purview and thus, could capture software developers who simply write and publish (or deploy) code. If this model were to be pursued, we respectfully request that HM Treasury explicitly define "establishing . . . a protocol" to exclude software developers and to only include centralised, intermediary-like activity.*

[16] Consultation § 11.7. *This also falls under the question of whether a DeFi protocol is "truly decentralised" or not; in the instance where there are centralised, identifiable actors, then those actors fall under a separate regime, even if the "services" they provide or the business they operate relates to a smart contract-based protocol in which users can engage in self-directed economic transactions.*

[17] Consultation § 11.8. *We are in favour of this approach and discuss it more extensively below.*

[18] *Id. We do not support blanket regulatory requirements on "front end" providers. A front end is simply a website; the website simplifies, but does not effect, various types of activities – some of which may resemble regulated financial services activity. Consistent with HM Treasury's intent to regulate "activities", any regulation of "front end providers" should focus on the activity the host operates or controls through the front end*

order to circumvent regulatory obligations should be subject to the same treatment as centralised organisations".[19]

It is critical that HM Treasury define "what" or "whom" it seeks to regulate when addressing certain risks that may arise from the use of DeFi protocols. Based on the Consultation's approach to reaching the "same regulatory outcome" for similar financial activities – along with the acknowledgement that "HM Treasury is looking for a proportionate, innovation friendly approach"[20] – we understand that HM Treasury seeks to mitigate risk in DeFi systems (to consumers and the market), ***not*** to regulate software developers who code and publish the software comprising DeFi protocols.

Although some of the models proposed in the Call for Evidence have been explored by others as potential methods for "regulating DeFi", we suggest below various regulatory frameworks that seek creative solutions to the unique challenges proposed by decentralised, software-based systems and protect the integrity of the software development process and allow for innovation (*i.e.*, not regulating "software development"), while simultaneously ensuring consumer protection and market integrity:

- Any FCA registered cryptoasset business, such as those discussed in the Consultation, that seeks to provide access to a DeFi protocol must provide representations to FCA regarding certain aspects of the protocol, including but not limited to (a) that the protocol had undergone auditing according to any industry standards or standards set by regulators; (b) the way in which the protocol is administrated or governed, including the existence of any administrative key and if one exists, who (not by name) or what holds it; (c) whether there are any emergency risk mitigation measures inherent in the code or otherwise (*e.g.*, a multi-signature wallet that has emergency powers and what those powers are); and (d) discussion of any hacks or scams associated with the DeFi protocol. The concepts set forth in (a) through (d) are suggestions based on accepted "best practices" in the industry and are not intended to be exhausted. This model is favourable because it maintains regulatory requirements with identifiable intermediaries. In addition, this model is likely to incentivize (i) better practices by software developers without directly regulating software development and (ii) more transparency about DeFi ecosystems. By requiring intermediaries to assume liability in undertaking investigations about DeFi protocols and providing representations about the same, software developers will be incentivised to create protocols that meet the standards intermediaries must certify (if they want intermediaries to plug into such protocols). In addition, intermediaries likely will make representations about DeFi protocols under one of two circumstances – they receive an indemnity from the software developer for any inaccuracy (or negligence or fraud) relating to representations made if they must rely on the software developer for the information – this scenario seems unlikely for a host of reasons; or all the necessary information is publicly available and verifiable – a much more likely scenario. Imposing regulation through this framework would not change the centralised intermediaries – typically "on and off ramps" – obligation to conduct Know-Your-Customer ("KYC") due diligence, to mitigate AML concerns.

[19] *See, e.g.*, Consultation § 11.7.

[20] Consultation § 11.10.

- Some regulators have suggested a voluntary "opt in" standards system through which a regulator sets standards for an "approved" DeFi protocol, including but not limited to cyber-security and audit standards, governance or administrative standards, etc. and to which anyone could provide an attestation and evidence that such DeFi protocol meets such standards to receive a "stamp of approval" from the FCA. This type of regulatory framework could be accompanied by a self-regulatory organisation ("SRO") in which industry participants, stakeholders and regulators work collaboratively to set industry standards. We favor this significantly over a mandatory standard setting regime, which will severely restrict innovation by preferencing better capitalized and established developers or prohibiting developers or coders to publish or deploy DeFi protocols from the UK or those that will reach UK users without undergoing a lengthy or expensive regulatory process.[21]

- As discussed in note 18 above, certain websites running additional backend infrastructure undertake ***activities*** that resemble or are identical to regulated financial activity, but occur entirely through algorithms or code. These "front end hosts" may or may not take fees from any transactions that occur on a DeFi protocol that occur through the front end. Regardless of whether any fees are collected, it is possible that, as the Call for Evidence recognises, that certain regulatory frameworks – like those for algorithmic trading – may be applicable. Such regulation would only apply to the hosts of these "front ends" and not at the protocol level.

We look forward to continuing to engage in collaborating with HM Treasury and in any additional FCA CryptoSprints on this issue.

Question 42. What other best practices exist today within DeFi organisations and infrastructures that should be formalised into industry standards or regulatory obligations?

Although we do not know precisely who or what is captured by the term "DeFi organisations and infrastructures", below we set forth a number of "best practices" employed by software developers building DeFi protocols that are believed to increase the safety and soundness of these protocols.

To mitigate both technology and cyber risk *before* a protocol is deployed, "best practice" includes robust auditing procedures – both internal and external to the development team. After code is written, it should be shared with other members of the internal team who did not write the code to review to find "bugs" or other vulnerabilities (including economic and technical); then the code should undergo auditing by a third party auditor who likewise vets and tests the code to determine any flaws; and then the software development team should consider the results of any outside audit and determine whether alterations to the code are necessary to ensure proper functioning. It is well-recognised by industry that code audits are critical to ensuring safe and effective operation of a DeFi protocol.

Third-party auditors play an important role in the safety and soundness of DeFi protocols; there are a number of reputable, well-known third party auditors as well as smaller auditors, all of

[21] Many of the most significant DeFi protocols today were developed by young coders, who originally had little to no funding. These protocols have operated well and have become a critical backbone to the DeFi ecosystem, but may not have ever been deployed under an arduous mandatory "standard setting" regime.

whom could play into the possibility of self-regulatory organisations (SROs) within the context of decentralised technology.

Despite the benefits of auditing, there are at least three helpful improvements in auditing practices that can be made: *first*, a standardisation of the approach to auditing smart contracts for DeFi protocols; *second,* a standardisation of when and how third party audits are used – *e.g.*, prior to launch, at the time of an upgrade to the code, etc; and *third*, standardising transparency around protocol audits will enhance accountability both for auditors and development teams, and will allow for even greater examination of the safety of code.

In addition, to mitigate cyber risk for protocols not yet deployed, developers can implement "gated" or "guarded" launches, which can be done in two ways: where the developer can restrict the protocol by limiting either the liquidity that can initially be injected into the system or the level of decentralisation for a limited time so quick updates can be implemented, or by restricting individual wallets by limiting the liquidity that a single wallet can contribute to the system.

Additional best practices for ensuring the safety of the code include, but are not limited to, bug bounty programs and "audit competitions". The former refers to programs where a software developer or a DAO offers rewards to individuals who find previously-undetected vulnerabilities in the code and privately disclose those vulnerabilities to the developer for correction. The latter refers to events where software developers offer rewards during a specific time to a specified (frequently identifiable) group of individuals who compete to find vulnerabilities in the code for correction before deployment of a protocol.

Finally, while not yet codified as a "best practice" or "industry standard", meaningful progress has been made with automated, technology-based monitoring systems for cyber risks. Such monitoring allows for the identification of suspicious on-chain activity, and triggers an emergency pause on the platform.

As with all parts of the DeFi ecosystem, the risk mitigation and monitoring tools continue to improve, such that current "best practices" outlined above are not comprehensive and will evolve over time. Accordingly, any contemplated regulation should be enacted with "regulatory outcomes" in mind rather than prescriptive requirements.

Other Cryptoasset Activities (Chapter Twelve)

Question 44. Is there merit in regulating mining and validation activities in the UK? What would be the main regulatory outcomes beyond sustainability objectives?

As a software developer who originally developed a proof-of-stake network, we respond to the question only as it pertains to validation. We do not believe there is merit in regulating validation activities in the UK and strongly encourage HM Treasury to engage in additional study before considering any regulation as it would pertain to validation activities.

Validation refers to technical activity for implementing a consensus mechanism that verifies transactions on a proof-of-stake blockchain network. It is not the type of "activity" contemplated under the UK's financial services regulation that exists today or under the proposed cryptoasset regulation set forth in the Consultation.

Validators are users who operate nodes that verify data and secure blockchain networks. As many have discussed, blockchain networks are communications protocols. Thus, verifying data sent to a blockchain network requires a user through a node (*i.e.*, a computer) to employ a set of mathematical principles to check the validity of the data provided to allow it to be recorded on a blockchain network.

Validation is intended to ensure the security of a proof-of-stake blockchain network by running software that maintains network data. When many individuals or entities validate the network data, then such data is maintained without the need for a centralised intermediary. Two mechanisms exist to incentivize an individual or entity to validate data properly and truthfully: (i) an individual or entity must commit – or "stake" – a certain amount of cryptoassets to the network so that they have cryptoassets at risk;[22] and (ii) the possibility to receive rewards for properly running the software and validating the data.

Some have suggested that validators may be intermediaries in blockchain transactions akin to traditional financial intermediaries. Others have suggested that validation more closely resembles the data systems underlying the current iteration of the Internet such that validators (a view with which we agree). At its core, validation is a data reporting and communications activity as well as a security activity ensuring the accuracy and truth of data on the network. If anything, such activity more closely resembles communications relating to financial transactions – ***not*** financial activity.

Further, it is important to note that not all transactions through applications deployed to a permissionless blockchain network are *financial* transactions; indeed, some of the latest blockchain-based applications have taken the form of social networks or consumer rewards programs. Validating such transactions would not necessarily have a financial component and thus, should not be regulated as financial or economic activity.

For all of these reasons, we believe validation is outside the scope of HM Treasury's proposed regulatory regime for cryptoassets – and should not be brought into the regulatory perimeter. Such regulation would have wide ranging implications and potential unintended consequences relating to technical data verification, including a breakdown of the natural processes underlying proof-of-stake blockchain networks, including the consensus mechanism, and possible censoring of the communication of data throughout the network.

We urge HM Treasury to engage in continued engagement regarding validation activities, including through industry and stakeholder roundtables, and to exclude any considered regulation of validation until significantly later stages of regulation, if it is to consider it at all.

[22] The term "staking" is currently used to refer to a wide variety of activities in the cryptoasset industry more than simply validating data on a proof-of-stake blockchain network. We believe a clear taxonomy relating to all types of activities that use this term – those that relate to validation activities for proof-of-stake blockchain networks versus those that refer to "staking as a service", "liquid staking" and "delegated staking" – will assist in assessing whether any such activity would constitute ***activities*** that require regulation. As noted above, "staking" in the form of validation should not be regulated.

Sustainability (Chapter Thirteen)

Question 48. What reliable indicators are useful and / or available to estimate the environmental impact of cryptoassets or the consensus mechanism which they rely on (e.g. energy usage and / or associated emission metrics, or other disclosures)?

The environmental impact of proof-of-stake consensus mechanisms mainly concerns three areas:[23] carbon emissions, energy use, and e-waste.[24] Energy use depends on the fundamental components of the technology including, hardware requirements, programming language, network size, transaction throughput and complexity, among others. This information, coupled with understanding who is using the technology (mainly miners and validators) and where (location of miners or validators, carbon intensity of electrical sources), would produce an estimate for carbon emissions.[25]

Question 49. What methodologies could be used to calculate these indicators (on a unit-by-unit or holdings basis)? Are any reliable proxies available?

To calculate the energy consumption of blockchain, there are two main approaches:[26] top-down (*i.e.*, assessing miners, block rewards, and transaction fees) and bottom-up (*i.e.*, assessing hardware and hash rate). The location of miners and validators is difficult to know for certain, but proxies, such as electricity costs in different areas and economic incentives of the blockchain itself, could be used to estimate the geographic spread and the electricity sources used.

Question 50. How interoperable would such indicators be with other recognised sustainability disclosure standards?

The environmental indicators mentioned above - carbon emissions and energy use - come from the OECD. Ways to quantify those indicators for blockchain may look different than in more traditional industries but would produce standardised numbers that are interoperable with current, recognised sustainability standards (*e.g.*, Greenhouse Gas (GHG) Protocol).[27]

Conclusion

We appreciate the opportunity to respond to the Consultation and the Call for Evidence and look forward to continuing to collaborate with HM Treasury on these matters. We believe the

---

[23] The OECD outlined a number of environmental indicators. The two mentioned here relate to the technology's *direct* effects. Other indicators may play a role for secondary or tertiary effects, but are not discussed in this response. (https://www.oecd.org/env/indicators-modelling-outlooks/37551205.pdf.)

[24] Although e-waste could be considered a factor for proof-of-stake networks, it mainly presents itself in proof-of-work networks. *See* https://github.com/Green-Software-Foundation/sci/blob/main/Software_Carbon_Intensity/Software_Carbon_Intensity_Specification.md, https://digiconomist.net/bitcoin-electronic-waste-monitor/

[25] For statistics and projects that have this information, *see* CCRI reports (*supra* n.11) *and* pp. 15-17 in the World Economic Forum report, *available at* https://www.weforum.org/reports/guidelines-for-improving-blockchain-s-environmental-social-and-economic-impact.

[26] *See* CCRI reports for more information on these approaches and methodologies for calculating the environmental impact of scaling solutions, *available at* https://carbon-ratings.com/.

[27] Please see the GHG Protocol website for more information, *available at* https://ghgprotocol.org/.

proposals set forward by HM Treasury are a significant step in establishing the UK as a “global cryptoasset hub”.

In the event HM Treasury holds hearings or meetings related to this Consultation and Call for Evidence, we would be pleased to participate. To the extent additional discussion or clarification of the points described above would be helpful, we would be happy to provide additional written materials or engage further with HM Treasury.