DAIMON LEGAL

Director - Crypto Policy Unit
Financial System Division
Treasury
Langton Cres
Parkes ACT 2600

**Sent only by email to**: crypto@treasury.gov.au

Friday, 3 March 2023

**Submission on Treasury's consultation paper – Token Mapping**

Dear Director,

Daimon Legal welcomes the opportunity to make this submission to the Consultation Paper issued by Treasury in February 2023.

By way of background, Daimon Legal provides legal services and advice at the cutting edge of fintech, emerging technologies and law, advising international clients in the DeFi, NFT, AI, cryptocurrency and blockchain industries. It has made contributions to numerous projects and law reform initiatives including those to establish Safe Harbour mechanisms for emerging DeFi and digital asset platforms initiated by Commissioner Peirce of the US Securities and Exchange Commission[1]. The author of this submission is also on the Board of the Dai Foundation, overseeing the operations and intellectual property for Maker DAO and is partner at AVentures DAO, a venture capital fund supporting DeFi and Game-Fi start-ups.

In this submission, the author does not represent any party other than himself and the views set out in the submission are the author's alone. They should not be relied up upon, and are not intended as financial or legal advice. On this basis, I respond as follows to the questions presented in the Paper:

**Q1) What do you think the role of Government should be in the regulation of the crypto ecosystem?**

The Government has a critical role to play in the development of regulations in relation to the crypto ecosystem. As has become apparent watching developments in other countries grappling with these issues, those jurisdictions that have shown a willingness to confront the novel legal and financial puzzles presented by emerging technologies and taking the necessary steps to develop and pass the relevant legislation have found themselves at a distinct advantage when it comes to capital investment, innovation and product development.

[1] See pull request initiated by Daimon Legal to Commissioner Peirce's github submission: https://github.com/Daimon-Law/SafeHarbor2.0

Taking the European Union as one example, while there has been some criticism of the proposed Markets in Crypto-Assets (MiCA) laws[2], the general consensus within the crypto, DLT and blockchain industry (Crypto Industry) is that the MiCA developments are welcomed as they are bona fide attempt to issue regulatory guidance based on a deep understanding of the technology, and provide a roadmap for investment and growth.

Market participants have been actively reaching out to, and collaborating with, government bodies and regulators, seeking to develop clear guidelines that provide certainty and allow for forward planning with respect to innovative business models. The common theme within the Crypto Industry is that regulatory clarity is taking longer than anticipated and any initiatives to expedite regulatory clarity is welcomed.

**Q2) What are your views on potential safeguards for consumers and investors?**

Australia has existing safeguards in place to protect consumers and investors in traditional market scenarios that can readily be applied to crypto tokens and other digital assets. The remedies available to both consumers and investors are adequate however is room for additional coverage when it comes to the categorisation of digital assets and whether such assets are covered by the existing regulatory measures.

Matters become more complicated in situations where there is no single party involved in the operation of the protocol or platform in which the consumer or investor is participating/investing. This is the case in respect of Decentralised Autonomous Organisations (DAOs), Decentralised Finance (DeFi) and network based games that have their own token economies and market. In these scenarios, it is not clear who the "owner and operator" of such platforms is, especially where the network rules governing the operation of such platforms is decentralised, global in nature and often governed by the users and network participants themselves.

The author notes that Treasury has, in its Paper, often relied on examples based on real-world games such as Monopoly, digital assets within a custodial setting and digitised assets. While these represent part of the ecosystem, they are not the primary part, nor are they representative of the direction the technology is moving in, which is towards greater decentralisation. The collapse of entities such as FTX, Celsius and Terra has reinforced the elevated risk associated with centralised and custodial solutions – both of which are subject to existing laws that provide promoters, consumers and investors with adequate remedies and regulatory clarity.

Digital assets defy easy categorisation (as noted in Annexure 1 of the Paper). For example, under the existing Australian consumer laws, protections are typically provided to "goods and services". Under existing legal frameworks, it remains uncertain whether digital assets will be viewed by the courts as "goods" or "services". The author notes that Treasury has considered the recommendations presented by the Law Commission of England and Wales (LCEW) in their Consultation Paper on Digital Assets[3]. In line with the recommendations

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[3] Law Commission of England and Wales "Digital Assets: Consultation paper" (28 July 2022) at https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2022/07/Digital-Assets-Consultation-Paper-Law-Commission-1.pdf accessed on 1 September 2022 (hereinafter referred to as the "Consultation Paper").

made by the LCEW, the author strongly recommends legislative reform necessary to confirm the legal basis for digital assets[4].

**Q3) Scams can be difficult for some consumers to identify.**

**a) Are there solutions (e.g. disclosure, code auditing or other requirements) that could be applied to safeguard consumers that choose to use crypto assets?**

The Crypto Industry frequently relies on code audits and white papers to provide insight into the safety and security of protocols and platforms. Code audits have proven to be less than effective in weeding out bad actors. This is due to a wide range of factors including auditor inexperience, complexity of the software code, ease with which audits can be circumvented as well as the difficulties in predicting the economic forces/game theory that are at play once the software has been launched in production. Software audits cannot, for example, identify the susceptibility of a platform to market manipulation or volatility although knowledge in this area is improving.

Disclosure requirements could be one useful area for increased rule-making. The author invites Treasury to consider the work done by Commissioner Peirce in her proposal for Safe Harbour arrangements under the *Securities Act of 1933* (US)[5] as one example of how the disclosure rules might apply to non-custodial market participants.

**b) What policy or regulatory levers could be used to ensure crypto token exchanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?**

In the author's recent interaction with crypto exchanges on behalf of clients, the on-boarding of tokens typically involves some effort to ensure that tokens and the teams that supply them are scrutinised although the sophistication of such scrutiny varies depending on the home jurisdiction of the exchange and the scale of the exchange's operations. As mentioned above, difficulties arise when it comes to auditing software, analysing the risks associated with the tokenomics of a particular token and the predicting the effects of market forces.

To take one example of LUNA and UST, while some academics had warned of the inherent, unavoidable risks associated with algorithmic stablecoins[6], the consensus in the Crypto Industry was that UST was based on a robust software platform, scalable and more than adequately collateralised. What the Crypto Industry and investors hadn't counted on was the *velocity* of "death spirals" in algorithmic stablecoins once the peg has been broken and the rapid drop of confidence in the underlying collateral - LUNA. In a similar fashion, the collapse of FTX was triggered to a large extent by FTX's reliance on its own token, FTT, as the collateral for loans taken out by FTX and its related investment arm, Alameda Research.

---

[4] See also the author's forthcoming article *Digital Assets and the New Jurisprudential Frontier in Property Law* in the Victorian Law Institute Journal (to be published April 2023)

[5] https://github.com/Daimon-Law/SafeHarbor2.0

[6] See Kluge-Mundt, Minca, *(In)Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks* https://arxiv.org/abs/1906.02152v3

That said, there is merit in standardising the criteria exchanges must apply when assessing risks associated with particular tokens. This should include software audits of the code and the provision of white papers setting out the details of:

- Tokenomics of the token, including:
    - the maximum supply of the token;
    - The distribution of the token amongst the founders of the project, seed and angel investors, stakers and validators, for liquidity providers, Treasury allocation, project team allocations and how the remaining balance will be distributed;
    - The vesting period, cliff and release schedule for each of the stakeholders mentioned above;
- The results of any software audit conducted and a certified copy report by the auditor who conducted the audit; and
- Any specific risks associated with that token and protocol, including with respect to liquidation of staking positions, risks of loss associated with BAU operations of the platform or protocol, the reliance on real world assets as collateral and details of such collateral.
- This should include a penalty regime for those knowingly supplying the exchange with incomplete or misleading information.

**Q4) The concept of 'exclusive use or control' of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.**

**a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation?**

The terms "control" and "excludability" have historically been used in the context of tangible personal property. This author contends that focusing on the 'rivalrousness' of a thing and defining this term will help courts determine matters quickly instead of looking to build analogues through the common law usage of 'control'.

Having reviewed the LCEW's consultation paper into crypto tokens and how existing proprietary rights should apply to such assets, this author has reached a similar conclusion to the LCEW that the concept of 'control' should, in the absence of stronger alternatives, be preferred over traditional definitions of proprietary rights based on 'possession' as this will provide greater clarity when defining and categorising crypto tokens.

It should be noted that even the concept of "control" becomes unstable when observing digital assets in a live production environment offered by smart contracts, DAOs or multi-signature wallets as it becomes harder to precisely establish excludability and control and distinguish between possession and control.

There is also an element of circularity in basing property rights around "control" of a thing. The LCEW felt the concept of control should therefore remain a higher level framing device. i.e. first establish property exists, then decide on control of such property where circumstances require one to do so.

Interestingly, the LCEW did not recommend reform to clarify the meaning of "control" and suggested the courts look to existing work by the UNIDROIT Digital Assets and Private Law Working Group to define how "control" might look in the context of digital assets.

Whether Treasury decides to further investigate the concept of rivalrousness as a suitable basis for crypto tokens and other digital assets, further work will be required to develop a model that helps stakeholders and the judiciary categorise digital assets and determine the legal rights associated with such things.

**b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?**

There are some obvious benefits of using existing formulas and legal theory to define crypto tokens and crypto networks where ready analogy is possible. Terms such as 'exclusive use' and 'control' are widely understood and accepted by the market, stakeholders and the legal system.

What has not been established at this stage is how those existing formulations would apply in the digital realm as there has been little case-law in this space. This represents a significant disadvantage in using existing frameworks to assess legal and proprietary rights associated with crypto tokens as it leaves market participants reliant on the common law to develop the necessary clarity as to how such concepts would apply to crypto tokens. This disadvantage is a key reason why this author advocates for legislative reform[7].

**Q5) This paper sets out some reasons for why a bespoke 'crypto asset' taxonomy may have minimal regulatory value.**

**a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?**

**b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?**

Taxonomies of technology such as crypto tokens are susceptible to obsolescence as technology develops. Simple examples of this type of obsolescence abound. One could have, for example, attempted a taxonomy of music media formats in 2010 (CD, LPs, Minidisc, mp3) that is barely recognisable today in an industry dominated by music streaming services.

We are already witnessing new forms of tokens and token types on a monthly basis. The theoretical underpinnings of crypto tokens is also being constantly challenged as the industry experiments with token forms representing identity and tokens that adapt over time or take on different functions in different contexts.

Even Treasury's own representation of token architecture (crypto token -> crypto system/asset -> function) is based on an increasingly dated, Turing-complete version of crypto tokens. The author predicts such architectures will represent a small part of the overall digital economy which will see increasing convergence of money and identity through such mechanisms as social scoring, underpinned by some form of

[7] See also the LCEW's recommendations in the Consultation Paper, 100-105.

cryptographically secured identity-value as the basis for both commercial and personal interactions/transactions. We have already seen the diminished role of physical money. In a future state, not only will physical money become obsolete but the relevance of money and traditional forms of legal tender will come under attack.

Notwithstanding the above concerns, the European Union's MiCA proposal demonstrates the benefits of developing a standalone regime in the short term (5-10 year horizon). It provides market entrants with a clear roadmap for the establishment and operation of crypto-native businesses and offers investors and the public the reference points and guidelines necessary for safe participation. Having a standalone regulatory regime "puts Australia on the map" in terms of technology investment.

As a counter-example, one could look at the impact in the United States caused by incremental judicial guidance on crypto-tokens, lack of regulatory clarity and the consequent heavy-handed response from regulators attempting to apply current laws to emerging fintech and crypto offerings. For many lawyers operating in the Crypto Industry (including the author), the United States is effectively a "no-go zone" for new crypto projects due to the risk of prosecution and insurmountable challenges when it comes to establishing and operating a crypto-native business. Of particular concern is the reluctance of US banks from dealing with crypto-native businesses due to regulatory uncertainty and the need to "read the tea-leaves" for guidance.

**c) In the absence of a bespoke taxonomy, what are your views on how to provide regulatory certainty to individuals and businesses using crypto networks and crypto assets in a non-financial manner?**

In the alternative, incremental adjustments and addenda to existing regulatory frameworks could be introduced so that Australia's functional approach to financial regulation can be enhanced while providing some measure of roadmap to market entrants. In the author's view, this approach is sub-optimal for the reasons set out above.

**Q6) Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real world assets.**

**a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?**

Reform is necessary in this space however the author queries whether a wrapped asset should receive the *same* regulatory treatment as that of the asset backing it. In these instances, the functional approach to regulation should be applied so that the regulations respond to the nature of the wrapped asset itself and how it functions and is used.

Gabriel Shapiro, a highly respected lawyer and jurist operating in the Crypto Industry explains as follows:

It is argued that digitization of ownership interests is beneficial but can be achieved without blockchain technology; however, blockchain technologies are uniquely suited to enhance the *individual asset sovereignty* of stockholders[8].

As Shapiro points out, accounting for asset sovereignty necessarily requires treating such tokens as bearer instruments which, in the Australian context, demands careful consideration for how such tokens will be viewed under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*. To take one simple example: if livestock were to be tokenized, would the related tokens be viewed as "bearer negotiable instruments" under s.17(g) of the Act and would farmers be expected to conduct KYC/AML and reporting in relation to the transfer of those tokens?

**b) Are reforms necessary to ensure issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens for the underlying good, product, or asset?**

Reforms could certainly respond to the uncertainties around provenance, ownership and re-hypothecation of assets. While it is arguable that existing laws provide some remedies (for example under the ACL or *Corporations Act*), the ease of tokenising real-world assets leads to increased risk for consumers and the market. Indeed, the author contends that such wrapped real-world assets are significantly more risky than purely digital assets – not only do wrapped assets inherit all the usual technological risks associated with crypto tokens but they add counter-party risks that are avoidable in a purely crypto context.

In traditional finance, such counter-party risks can be mitigated by way of contractual agreements, escrow arrangements and trusted intermediaries. However tokenisation or wrapping, from a technical standpoint, does not require any of these things. It requires no disclosures, contracts or remedies to be created. Moreover, the underlying connection of tokens to their real-world asset cannot be readily enforced by the on-chain mechanisms typically available in crypto-native transactions such as those offered by DeFi applications.

Consequently, wrapped real-world assets need real-world law to underpin them. This could include regulations addressing disclosure requirements, provenance guarantees and *de minimus* contractual provisions/protections. Such regulations should also address the custodial/agency issues, including with respect to the proprietary nature of the wrapped asset and how title of the token and underlying real-world asset will be determined in various settings (for example, under the *Personal Property Securities Act 2009*).

[8] Gabriel Shapiro *Representation of Corporate Capital Stock via Cryptographically Secured Blockchain Tokens: Motivations and Potential Implementations* https://gabrielshapiro.wordpress.com/2018/10/28/2/

**Q7)** **It can be difficult to identify the arrangements that constitute an intermediated token system.**

**a)** **Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved?**

The simplest way of achieving this would be for CASPs to provide the same level of detail provided to them by the offeror. Where crypto tokens are developed by anonymous teams or by DAOs lacking the requisite information, the CASP should indicate which information is missing and how this impacts the risk profile of a token so that users can assess risk prior to making a decision with respect to such tokens.

**b)** **What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?**

Education of market participants (at all levels) remains a concern and CASPs have a unique role to play because they are often the first interaction a new user has with crypto tokens. Even seasoned users of crypto tokens and systems have underplayed or forgotten the distinction between custodial and non-custodial arrangements and how they affect risk. There are very few recent examples of crypto tokens being misappropriated from a user's own non-custodial wallet however there are countless examples of tokens being stolen, hacked, re-hypothecated in risky fashion, loaned without sufficient, or any, collateral or simply lost in circumstances involving custodial arrangements (such as where tokens are held by CASPs, other intermediaries, centralised apps or similar arrangements). CASPs should be transparent about this risk.

Memes have played an important role in the growth of the crypto economy with core messages such as "not your keys, not your coins"[9] – messages which resonate powerfully today in the wake of the collapse of numerous custodial service providers such as FTX and Celsius. These cornerstones of crypto token usage should be mandatory components of any education program, whether conducted by regulators or CASPs.

**Q8)** **In addition to the functional perimeter, the *Corporations Act* lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.**

**a)** **Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?**

As stated above in response to Question 5, the author recommends against regulation of specific crypto assets as this will lead to rapid obsolescence. There is also the difficulty in defining such crypto assets in a way that is technology-neutral.

[9] Popularised by Andreas Antonopoulos - https://cointelegraph.com/news/antonopoulos-your-keys-your-bitcoin-not-your-keys-not-your-bitcoin

**b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?**

The author concurs with Treasury that Australia's functional approach to regulation should be maintained where possible. This includes with respect to intermediated and custodial goods and services involving crypto assets and tokens. One area that remains unclear and requires further work from a regulatory standpoint is the legal recognition of crypto tokens and crypto assets – whether as "property" or "money". This clarity will enable service providers to respond accordingly in their dealings with such tokens and assets.

**Q9) Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?**

The suitability of public networks should be assessed on the following basis:

- Security of the network in terms of:
    - demonstrable security of the consensus layer in the network stack;
    - the distribution/decentralisation of validators/nodes/stakers;
    - the extent to which the network has experienced prior security incidents affecting the consensus layer; and
    - the ability of core developers to respond to incidents affecting network availability and security.
- The ability of the network to protect the privacy of users in their dealings with intermediated crypto assets.
- Demonstrable performance with respect to transaction throughput and transaction finality (transaction speed that does not account for transaction finality is a misleading figure. Finality, meaning the point at which a network confirms a transaction as irreversible and immutable is an important criteria as blockchain confirmations can vary between sub-seconds on some networks versus hours or even days on others).
- Transaction costs – some networks, including established public networks such as Ethereum, remain prohibitively expensive for all but the largest of transactions and are unsuitable for regular users.

**Q10) Intermediated crypto assets involve crypto tokens linked to intangible property or other arrangements. Should there be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework? Why?**

The author refers to the response to questions 6 and 7.

**Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?**

The marketing of crypto tokens and crypto assets is an area certainly requiring further clarity. Under existing arrangements, it is not clear whether marketing of crypto tokens and crypto assets is akin to marketing traditional financial products, particularly in respect to intermediated crypto goods and services. This will be less of a concern if some of the abovementioned reforms to clarify the legal recognition of crypto tokens and assets are implemented.

The author remains skeptical regarding the use of product disclosure statements which are rarely useful to average users of financial products and can often obscure the true risks. Part of this stems from the fact that all risks can be treated equally in the PDS with no requirement to identify *likelihood* of such risks. Crypto tokens and assets, particularly in a custodial/intermediated setting have very specific risks beyond those borne by market conditions and market volatility. They should not simply be added to a traditional PDS and should instead be highlighted in any disclosure/marketing.

**Q12) Smart contracts are commonly developed as 'free open-source software'. They are often published and republished by entities other than their original authors.**

**a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?**

As a market participant who advises and supports development of crypto projects, a recurring theme when identifying suitable jurisdictions is the ability to establish a low-cost, light-touch regulatory regime that allows projects and businesses to establish themselves as a going concern.

Many projects the author has spoken with are open to compliance with local regulatory frameworks but frequently object to the costs associated with such compliance and unpredictable behaviour by regulators as prohibitive factors. Banking and insurance are also of concern for many projects as they grow their business and move from informal development of open-source software to more formal/centralised software development as this path requires interaction with traditional financial rails which rely upon KYC/AML requirements that can only be satisfied if the project team is properly established.

Some jurisdictions have experimented with regulatory sandboxes which Treasury may wish to consider. The author supports the idea of regulatory sandboxes if they are cost effective and flexible enough to accommodate micro businesses and small-medium enterprises. The sandbox should also provide a cost-effective transition to the wider regulatory regime. Too often, this transition process is not effective and results in projects conducting regulatory arbitrage or moving offshore at the end of the sandbox period.

More effective than a regulatory sandbox is ensuring that the regulatory framework holistically accommodates micro businesses and SMEs, perhaps by way of “incubator” mechanisms that are based on capital/revenue thresholds.

**b) What are the regulatory and policy levers available to ensure smart contract *applications* comply with existing regulatory frameworks?**

Historically, *publicly* available software has rarely been subject to successful regulatory responses. One could perhaps look at the examples of protocols such as eMule and Bitorrent for parallels however any regulatory action taken against the promoters of such protocols has simply spawned copycats and more robust protocols that are less susceptible to regulatory action.

More importantly, the innovations developed by such protocols (including the quantum leaps in understanding distributed networks and distributed ledgers) have been beneficial in legitimate use-cases such as streaming services and communications tools. Those innovations led directly to the creation of Bitcoin and subsequent crypto tokens as well as many other online services used today.

This question also extends beyond financial regulations into legal principles of agency, tortious conduct and criminal liability. It is beyond the reach of this submission to analyse the legal mechanisms and policy levers across this spectrum.

**Q13) Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. only recourse in the event of default is the collateral).**

**a) What are the key risk differences between smart-contract and conventional pawn-broker lending?**

There are numerous differences between these forms of lending, the primary difference being the elimination of counter-party risk when using smart contracts and removal of any uncertainty regarding repayment of the associated debt. Payments and all other transactions in relation to the loan are traceable and independently verifiable.

Smart contracts further reduce the risks associated with such loans as it is possible to open up novel revenue streams and profit-sharing arrangements associated with the underlying asset. Repayments can be automated, and loan transfers are simplified by way of smart contracts – each can be done without further input from the counter-parties. As these loans are fully collateralised, smart contracts open up novel financial derivatives, reducing loan periods and the interest payable.

**b) Is there quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for analagous services provided through smart contract applications?**

The author is not aware of blockchain-enabled pawn-broking services being offered in a common law jurisdiction although one could argue that decentralised lending platforms are already analogous to pawn-broking given the comparable loan-to-value ratios. Pawn-broking is an emerging use-case in the crypto sector, principally focused on digital assets as the collateral for loans. Greater legal clarity on the proprietary nature of crypto tokens and crypto assets backed by real-world assets will naturally lead to increased competition in the pawn-broking sector, similar to the increased use of payment services that resulted from the shift away from physical cash to electronic payments.

Despite the lack of examples of "pawn brokers" in the digital realm, the performance of decentralised lending services more broadly (such as those provided by AAVE and Maker DAO) as measured against their permissioned, centralised counterparts over the past two years provide ample evidence that decentralised, permissionless lending systems built on public, open source blockchains provide *increased* protection for consumers against adverse market conditions and black-swan events.

**Q14) Some smart contract applications assist users to connect to automated market makers (AMM).**

**a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange?**

As with the pawn-broker examples above, the primary difference between AMMs and centralised exchanges is the elimination of counter-party risk when using smart contracts and removal of any uncertainty regarding trades. Payments and all other transactions in relation to trading positions are traceable and independently verifiable.

Unlike the pawn-broking model, use of AMMs introduces risks that do not have ready counterparts in centralised exchanges (without some form of collusion and market manipulation). Some of these additional risks are as follows:

- AMMs open up increased risk of front-running and sandwiching of trades, leading to reduced price transparency. This loss of value (actually a transfer of value associated with trading activity from traders to miners/validators commonly referred to as miner extractable value or MEV[10]) has become its own industry as various stakeholders involved with supporting the operation and security of crypto networks compete to extract value from trading activity by way of manipulating the order of trades, interposing trades or taking advantage of other exploits to benefit from price slippage and price movement.
- Research on the current model of AMMs based on constant function market making liquidity pools (such as those used by the large majority of AMMs) suggests that privacy of trades is near impossible[11] and attempts at obfuscation of trades leads to degraded user experience and safe functioning of the AMM[12].

**b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?**

The author is not aware of consumer surveys offering such comparisons. There is some literature providing comparative analysis of the respective performance of

[10] Daian, Phillip, Goldfeder, Steven, Kell, Tyler, Li, Yunqi, Zhao, Xueyuan, Bentov, Iddo, Breidenbach, Lorenz, Juels, Ari (2019). "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges". arXiv:1904.05234v1.
[11] Guillermo Angeris, Alex Evans, Tarun Chitra. *A Note on Privacy in Constant Function Market Makers* arXiv preprint arXiv:2103.01193, 2021.
[12] Ibid at 11.

AMMs and centralised exchanges[13][14] however the popular usage of AMMs is a relatively recent phenomenon[15] with insufficient historical data to reach statistically reliable conclusions or form the basis for policy decisions.

I would like to thank Treasury for providing an opportunity to respond to this important initiative. Please do not hesitate to contact me should you wish to discuss any of the issues raised in this letter.

Kind regards,

[13] Barbon, Andrea and Ranaldo, Angelo 2022 "On The Quality Of Cryptocurrency Markets - Centralized Versus Decentralized Exchanges", arXiv:2112.07386v5.
[14] Qin, K., Zhou, L., Afonin, Y., Lazzaretti, L. and Gervais, A., 2021. CeFi vs. DeFi--Comparing Centralized to Decentralized Finance. arXiv preprint arXiv:2106.08157.
[15] One could argue that AMMs only came to prominence during "DeFi Summer" which commenced in April 2020.