Magnet Capital

1st March 2023

Director – Crypto Policy Unit
Financial System Division
The Treasury
Langton Crescent
PARKES ACT 2600

Submitted electronically to crypto@treasury.gov.au

Submission to the Treasury in response to their February 2023 Token Mapping Consultation Paper

About Magnet Capital

Magnet Capital is a crypto-native digital asset investment manager, providing Wholesale investors with tailored exposure to a new asset class. Launched in 2017, Magnet Capital has a track record of over 5 years of market outperformance, driven by our ability to capitalise on the unique challenges and opportunities inherent within the digital asset ecosystem.

Preface

The Treasury Department's recent Token Mapping Consultation Paper highlights the Australian Government's efforts to understand some of the issues faced by regulators as they endeavour to interface with crypto assets. At a high level, it does a good job distilling complex aspects of the crypto industry and token design into simple to understand themes and categories.

However, the overarching approach of focusing on function and remaining technology neutral fundamentally overlooks core attributes that make blockchain such an attractive technology.

We appreciate the immense challenges associated with framing regulations for a new technology. **But we believe this approach bypasses the more critical step of outlining the foundational approach to effectively regulating decentralised networks. Instead, we suggest that Treasury commence work on defining a reporting standard that takes advantage of the inherent transparency of blockchain technology.**

The existing approach is likely to result in restrictive and impractical frameworks and policies that will drive crypto entrepreneurs, innovation and services offshore, without materially improving regulatory outcomes.

Australians have proven a strong desire to access crypto products and services, evidenced by us having the third highest rate of adoption in the world[1]. Without the optionality to access desirable products and services locally, Australians will continue to engage with offshore alternatives. The risk for regulators is that desirable products and services operate in less regulated jurisdictions with less accountability and where Australian regulators have no oversight or transparency.

As noted in the Consultation Paper, blockchain technology possesses "interesting properties in terms of efficiency, transparency, accessibility and composability", many of which aid regulators in their endeavours to ensure "markets are fair, efficient and competitive".

We take this one step further and note that crypto networks and assets that operate on public blockchains have transparent records of all accounts and cryptographically proven balances. Additionally, every transfer can be observed and witnessed and even complex financial products (e.g. derivatives) are defined transparently. Most importantly from a regulatory perspective, all this information can be obtained in real-time, and for free, not through expensive Bloomberg, Capital IQ or Factset subscriptions. The rules of engagement for crypto networks and assets work exactly as written with no human subjectivity, removing the need for any concern of execution. These are just some of the powerful characteristics that blockchain technology permits.

This technological innovation is highly friendly to regulators. Regulators should endeavour not to retrofit existing regulation as a first step, but should strive to leverage the power of open and permissionless networks to their advantage. Some examples of how this technology overcomes closed business operation :

- **Financial reporting:** Protocol revenue generation and expenditure can be monitored in real-time, improving financial reporting from a semi-annual, backward looking, point-in-time perspective, to a live view.
- **Solvency monitoring and custody controls**: Regulators can monitor the solvency and custodied assets of a decentralised protocol in real-time, unlike FTX[2] (or any other centralised exchange) where solvency issues and gaps in assets in custody are generally only discovered once they are catastrophic.
- **Capital ratio requirements**: Capital adequacy ratios are codified to protect crypto network users, this has prevented networks like Aave and Compound being subject to the risks that ultimately resulted in Genesis[3] and BlockFi[4] declaring bankruptcy.

[1] Cryptocurrency in Australia: 7 Key Charts & Statistics
[2] The Epic Collapse of Sam Bankman-Fried's FTX Exchange
[3] Crypto lender Genesis files for bankruptcy
[4] BlockFi Had $600 Million in Crypto Loans Not Covered by Collateral in Q2

- **Re-hypothecation of assets:** Codified and immutable rules that define how customers can be utilised prevent assets being misused. This has prevented crypto networks such as Aave from betraying user trust and losing customer funds as was the case with Celsius[5].

Critically, this allows for an improved, real-time source of reporting on business activity, performance against stated objectives, fairness of consumer engagement, financial health and solvency for all market participants.

Due to the immutable, transparent, permissionless, open nature of decentralised applications built on blockchain technology, many of the existing regulations designed for centralised businesses which have limited transparency are perhaps unnecessary and impractical. For example:

- On-chain protocol revenue and expenses can be publicly observed in real-time. This is in contrast to the current regulatory regime which only requires they be publicly disclosed to shareholders via periodic reports.
- Prudential regulations such as assets and liabilities balances, capital adequacy, solvency and liquidity measurements are publicly disclosed through smart contracts and their enforcement is verifiable and auditable in real-time via the public codebase/blockchain ledger. This is in contrast to private companies who have historically required regulatory oversight due to businesses failing to disclose risky practices or insolvency until it was too late for unknowing customers/investors to exit without loss.

In short, why not design a regulatory framework that harnesses the benefits of this transparency (i.e. by mandating a standardised structure for live on-chain reporting) and compliments regulatory objectives rather than retrofit the existing regulatory structure.

By interjecting legacy regulations that are not fit for purpose nor practical within this industry, it pushes innovation, opportunity and businesses to offshore venues with lower or no regulatory oversight, limited accountability and non-transparent disclosures of risk.

Problems with the existing approach

Public blockchain infrastructure is global and permissionless by design. This means that anyone, anywhere can launch their own crypto token/application with a few lines of code. One's ability to interact with this permissionless code on a public blockchain infrastructure cannot be prevented by regulators. Similarly, regulators cannot prevent users from accessing information (or misinformation) on the internet given that it is a global and permissionless public infrastructure. Both can be hindered through geoblocking and other measures, but complete prevention is near impossible.

[5] Celsius bankruptcy filing

Herein lies a regulator's biggest issue. Similarly to information on the internet, pragmatic approaches can be taken to ensure protection for constituents that operate within recommended and regulated products or frameworks.

The utopian goal is to provide a 100% secure and safe environment for blockchain users. But the reality is that bad and fraudulent actors will operate on any public technology infrastructure regardless of regulatory oversight, just like they do on the internet. Designing to overcome the edge cases likely only impedes the good actors and stifles innovation within your jurisdiction.

Rather than trying to design regulation to prevent the scammers and fraudsters from operating under the government's guise, why not provide an accommodative and sensible environment for the good actors to thrive.

This leverages the same premise as not acting as gatekeepers to all information published on the internet. But rather promoting and encouraging regulated and reliable sources of information so that they can thrive and service local constituents.

An alternate approach to crypto asset regulation

Crypto asset regulation is not easy. Magnet Capital does not pretend to hold all the answers. Just suggestions that we hope can be met with productive commentary to get towards a mutually beneficial goal for regulators. The crypto industry and ultimately Australia.

The Consultation Paper outlines a path to regulating crypto assets which starts with their categorisation and likening them to traditional financial functions. Whilst many crypto tokens/applications be categorised as such, given their operations take place on a public open ledger, **should we require the same regulatory oversight as we do for centralised businesses which have limited transparency?**

A core reason why rules and regulations exist is to create transparency and accountability where it does not exist. In truly decentralised public blockchain applications:

- Rules of operation can be verified by anyone, including regulators, in real time
- Solvency can be verified by anyone, including regulators, in real time
- Asset utilisation can be verified by anyone, including regulators, in real time
- Revenues can be verified by anyone, including regulators, in real time
- Treasury/DAO balances can be verified by anyone, including regulators, in real time

Fundamentally, blockchain based crypto assets are regulatory friendly by default due to their transparency. Regulators should leverage this design principle to their advantage and design regulatory approaches and frameworks accordingly.

Due to this, we believe a regulatory framework should be built from the ground up with this in mind, rather than adapting existing systems which may lead to reduced regulatory effectiveness. Without understanding how Treasury plans to move forward from here, perhaps a better starting point would be to seek to determine a means by which regulators can effectively regulate centralised (and eventually decentralised) crypto asset service providers. For example:

- Require product and asset disclosures on centralised service provider products
- Design a framework for what constitutes a sufficient level of decentralisation for a product/service to be considered a 'decentralised service provider'.
- Determine audit requirements for crypto assets listed by Australian product/service providers.
- Require on-chain ledger and statements for auditors to check validity of marketing material, PDS's, solvency, etc.

Centralised Crypto Asset Service Providers

A potential starting point which can create quick and measurable outcomes is to ensure that financial service providers that intersect with crypto abide by a basic regulatory standard in line with traditional markets. Crypto exchanges and third party custodians should align with the requirements that traditional financial market service providers have to align to. No more hiding behind the facade of 'crypto is different' and 'the regulator doesn't *yet* require me to'.

These businesses operate locally, have executives and directors within the country and perform nearly identical operations to traditional non-crypto counterparts.

Initially, do not impose strong restrictions on services provided, nor become an autocrat determining what assets can and cannot be listed on their platforms. Allow these businesses which currently possess significant knowledge of the industry to self select their assets/services. But, require them to report in a way which can promote diligence, accountability and a collaborative process with regulators. For example require a standardised application process which ensures a detailed enough level of diligence, and a period of commentary from regulators (not restrictions), before service providers list new assets or launch new services. More detail on these ideas below in *A Suggested Path Forward*.

Decentralised Crypto Asset Service Providers

If one acknowledges that open permissionless infrastructure means that any global participant can launch a public blockchain based product/service or interact with any product/service, then prevention should be the goal, not elimination, as it is unrealistic.

Elimination or severe restrictions locally will ultimately result in users seeking offshore venues to access the products they wish to engage with. This leaves them susceptible to fraudulent actors that operate in underregulated jurisdictions and also susceptible to engaging with scam or scam-like operators whose projects get listed by service providers outside of Australia.

As such, just like regulation for internet businesses, why not let the credible, accountable local businesses determine what are the right assets to safely and securely offer? Just like the AFR wouldn't intentionally publish scam advertisements and harmful misinformation, nor would we expect a licensed local exchange to knowingly list crypto scams and fraudulent tokens (otherwise risk business and/or personal repercussions).

This style of regulation that has worked effectively within the information industry could equally work as effectively in the crypto industry. Regulating email is a futile endeavour, whereas regulating Google is possible and effective.

Permitting the centralised providers of services to self regulate is the most efficient and effective manner for regulators to operate. Should centralised service providers promote scam and/or fraudulent crypto assets, they would face investigations, fines and/or criminal actions just like a media company that started publishing hate crimes and scams might.

Throughout a period of learning, a safe harbour perhaps, regulators can learn from local businesses to better inform future policy decisions. A prolonged learning period seems prudent in such a nascent industry so not to set precedents and policies prior to fully understanding how the industry evolves. Such an approach can enable regulators to ultimately determine what is sufficient enough for an open sourced and public blockchain application to freely be available to the Australian public. For example:

- What measurements determine whether a service provider is centralised or decentralised?
- How many audits does a decentralised code base require (if any) before being safe to be made available to the Australian public?
- What disclosures around token economics and vesting schedules are required?
- How long does a decentralised application have to meet these conditions? (assuming most of these are unrealistic expectations from day 1)

A Suggested Path Forward

Pause the token mapping exercise - commencing work with a token mapping exercise that fails to articulate how Government can effectively engage with a permissionless and globally distributed technology will not achieve the desired outcomes. This is because retrofitting existing policy frameworks by a crypto asset's function overlooks the different capabilities of blockchain technology that underpins crypto. Even if the function served is the same, blockchain can increase transparency, increase reporting frequency (to real-time), improve

efficiencies and codify fairness. Overlooking technology overlooks these characteristics that aid regulators in achieving their stated outcomes.

When more time has been spent to better understand how crypto assets functionally operate and how the industry is evolving (through more industry engagement and closer observation of crypto communities), the correct form of token mapping may prove to be an effective exercise (e.g. mapping to asset class such as commodity, currency, security, loyalty, etc)

Regulate centralised financial service providers under (mostly) existing frameworks - work to ensure local investors receive protections where they are most vulnerable. Most investors access crypto markets through a centralised financial service provider. Most of 2022's failures were those of centralised financial service providers.

Create a safe harbour for centralised financial service providers - work with the on and off ramps into the crypto industry to define standards and to work on building industry disclosures and transparency. **Provide them with a safe harbour to encourage innovation and industry growth without fear of uncertain regulatory backlash.** During this period, require a determined level of reporting so that regulators can learn how the industry operates and understand how it is evolving.

Require more disclosures from centralised financial service providers to the investing public - An example could be to require exchanges to curate documentation for each asset they list, akin to a prospectus for an IPO. This could include information including:

- Description of the asset
- Technology on which it is built (e.g. Ethereum, Binance Smart Chain, Avalanche, etc).
- Known or unknown status of team members and/or core contributors
- Token economics - total supply, distribution, escrow schedule, known large holders
- Historical price, market capitalisation and daily traded volume on credible exchange venues
- Key risks of the product
- Size of project treasury and what assets are held in the treasury
- Any relevant on chain metrics that may indicate utilisation of the product or aid in informing an investor of the projects adoption
- Publicly disclosed information on the project's roadmap
- Share public audits conduction on the codebase
- Level of decentralisation - e.g. who changes the code? Who can access treasury assets? Who governs the application/protocol?
- Create dashboards to monitor on-chain health and progress (e.g. monthly active users, transaction volume, fees paid/collected, etc)
- Etc.

Defining reporting structures for crypto assets - dependent on the operations of a protocol, reporting standards could be defined to help improve disclosures, increase customer

understanding and allow investors to make more informed decisions. Examples of on-chain metrics that might help improve disclosures and enable more informed decision making include; transaction volumes, number of transactions, number of addresses with assets, top 20 holder distribution, report protocol revenues, treasury balances and treasury cash flows. Note: differing categories of crypto assets will have different metrics that are more/less relevant to them.

Further steps to be determined at a later stage - without greater understanding and knowledge of how this industry evolves, more information is required before going much further than the above.

Conclusion

Simplified, a regulator's role is to design frameworks and policies that promote a healthy, fair, efficient and competitive environment, then ensure that businesses abide by those measures. Relative to non-transparent business operations, many crypto businesses / applications that exist on public and transparent blockchain ledgers aid in a regulator meeting their objectives!

Simply applying existing financial frameworks to a new asset class and hoping the retrofit will work, is a misaligned approach to creating security for participants.

Throughout a prolonged process of discovery and industry partnership, such as the one detailed above, the hope would be that a regulator can attain an intimate understanding of the complimentary ways to work with and design policy for public blockchains and decentralised applications. Technology neutrality works if the underlying principles of the foundational protocol are the same (e.g. operating systems built on http). But when the foundational protocol is functionally different (e.g. blockchain vs http), a different approach, new policies, new regulation and updated frameworks are required for regulators to effectively engage and create a welcoming environment for innovation and entrepreneurs locally.

Specific Responses to Consultation Questions

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

Answered above, but in short - Currently Governments should be focused on regulating centralised crypto asset service providers effectively. These were the most damaging businesses to consumers in 2022. This means working with service providers to design frameworks and policies that ensure more accountability and greater conformity with relevant existing financial regulations.

Government's role should be creating the guardrails upon which businesses can operate without the fear of regulatory ramifications. As an example, local exchanges and even traditional financial institutions (e.g. banks) should be allowed to safely provide on-boarding and off-boarding services to crypto assets that pass their internal risk frameworks. This would ensure Australians engaged with a trusted and highly respected entity, rather than needing to seek out services of un- or under-regulated offshore entities.

Throughout a multi year process of discovery and work with industry participants (e.g. safe harbour), Government should continually evolve their thinking and learn the most effective ways to engage with decentralised crypto assets/applications.

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

Answered above, but in short - Focus on protecting consumers and investors where they most frequently engage, through placing the onus on centralised financial service providers to only list credible assets.

Additionally, significant educational efforts, most likely conducted by centralised financial service providers, can help consumers engage more safely within decentralised systems (e.g. a trust score for decentralised applications or on-chain reporting standards).

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?**
>
> Centralised financial service providers should absolutely be required to have disclosures on products they offer and assets they list. These disclosures could include items like product disclosures, use of funds, risks associated with products. They could also provide disclosures for crypto assets they provide services for - public audits conducted, known team members, market capitalisation, historical performance (both price and technical), relevant on-chain metrics, links to public research, etc.

Just like blogs mostly don't have self-written disclosures on the accuracy of content provided, it is unlikely regulators will have the ability to require decentralised protocols to write their own disclosures (although some already do!).

Stopping constituents investing in scams comes down to empowering local and accountable service providers and improving investor education across crypto. It is difficult to regulate how Australians choose to spend their money, particularly in a global permissionless environment, but the Government can provide best practice when doing so.

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?

Answered above, but in short - require centralised service providers to conduct documented diligence on any asset they provide services for. This will not prevent all scams (just like an ASX listing does not definitively mean a company isn't mismanaged), but should prevent the majority from being listed on high quality local service providers.

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?

Decline to answer.

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

Decline to answer.

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?

A taxonomy such as the one proposed will be of limited assistance to regulators seeking to engage with truly decentralised crypto protocols. Regardless of their function, regulatory oversight and policy/frameworks put in place for code that lives autonomously on a public network are near impossible to enforce. Perhaps a different

taxonomy would be more fitting. But per commentary throughout this submission, we suggest a different starting point until a time at which categorisation of assets will aid in meeting regulatory goals.

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

Decline to answer - it is too early in blockchain and crypto's lifecycle and regulatory discovery to try to be answering this.

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?

Understand the vectors of harm that these protocols can inflict. Mostly this comes down to the level of decentralisation of a protocol and strength of the code base. If a single actor can change the code or access the treasury, they can single handedly ruin an application/token and harm customers in the process. In the case of Bitcoin this cannot happen as there is no single centralised source that can change the code, or has access to development, or can drain funds from a treasury (granted this wasn't the case on day 1 and took time).

In regards to hacks and economic exploits of crypto networks and assets, perhaps audit requirements, length of existence and other measures can be taken to ensure protocols that are available to Australians have become robust to such threats.

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?

Cash is a promissory note. Wrapped real-world assets are promissory tokens. The issuer of the token should be regulated to ensure they maintain solvency and maintain the assets they purport to own. Then depending on the real world asset, there should be varying degrees of regulation that align with their traditional counterparts.

- Stablecoins are digital cash. In the first instance, just like cash, the existence and transfer of digital stablecoin should not be regulated. Benefits of a stablecoin relative to cash is the presence of a public digital record of all activity. As such, unlike cash, usage can be restricted if it is identified as being utilised in nefarious ways (through blacklisting policies[6]). Policies such as

[6] Circle Blacklisting policy

acceptance of stablecoin over a threshold value (i.e. $10,000) as a means of payment require reporting to AUSTRAC[7].

- Wrapped real-world assets that require registration (e.g. Property and public equities) might require 'allowlists'. Which function to only permit registered addresses receive and transmit particular digital representations of real-world assets.
- Wrapped real-world asset issuers are similar to custody providers and could be regulated in the same way.

The purpose of such examples above is to demonstrate there are practical solutions that can leverage blockchain and crypto solutions to serve similar functions (maybe even enhanced) to their real world counterparts. However, the point where most regulation will be required is at the issuer level of such assets as that is where transparent code and registers don't exist.

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?

Yes. But we are unsure what those specifically are without further diligence.

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?

Yes - suggestions as to how this can be achieved are detailed above. Some requirements might not have to be done independently but in partnership with an independent entity (e.g. just like credit ratings are provided by Standard and Poors, an independent crypto research agency can provide commentary or metrics to better inform customers).

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

Suggestions as to how this can be achieved are described above (e.g. education, disclosures, on-chain metric visibility).

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.

[7] Reporting transactions of $10,000 and over

Per above perspectives, categorisation like this is unnecessary as the first step of regulation. Could be revisited later.

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

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

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?

In the first instance and until deemed otherwise, the issuer of wrapped real-world assets should restrict their usage in line with existing regulatory requirements until a time when open permissionless interaction is deemed appropriate. An example of this is that if Australian public equities were wrapped by a centralised entity, the ownership of such assets should abide by the same KYC/AML requirements that a non-wrapped version should (i.e. encode an allowlist where only addresses that are registered to a known and approved identity can transact with the wrapped real-world asset).

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?

Hard to classify all assets together here. No comment without further clarity as to what intermediated crypto assets are being considered here.

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?

Similar requirements should be in place for traditional investment advice or promotion. Anyone promoting a financial investment should disclose their position, the terms under which the position was acquired and the intention of their holding.

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?

For centralised entities utilising public blockchain networks to develop business solutions there may be a few levers that could be pulled (specific to each industry / function and therefore difficult to detail here).
However, doing so might render it difficult for them to compete with decentralised counterparts (where they don't have an inherent advantage for example rights to tokenise Australian public equities due to the associated custody and KYC requirements a decentralised counterparty could not overcome).

For operations that are controlled decentrally or operate outside of Australia I'm unsure there are many levers that would be effective given the global and permissionless nature of blockchain technology. I'd assume an analogy that effectively demonstrates the difficulty would be considering the regulatory requirements to encourage digital publishing of information that comply with pre-internet media regulatory frameworks.

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

Similar comments to the above in 12(a)

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?

The analogy to pawn-broking is a peculiar one. Pawn brokers can misguide or trick customers through a variety of mechanisms (predatory practices have resulted in mispriced collateral, unfair loan requirements depending on customers conditions/desperation, seizure of the entire collateral position should strict or unfair conditions not be met, etc).

A better analogy might be to compare them to margin loans offered by share brokers. Publicly traded equities carry a live market price that is transparent, loans are mostly overcollateralised and any residual value post pre-defined break fees is returned to the borrower if margin called.

None of the above described pawn broker scenarios are possible in reputable smart contract applications (e.g. AAVE or Compound, the largest smart contract applications of this type). Such instances, like margin loans on public equities, accept fungible collateral (unlike a pawn broker), provide the same lending conditions to all users (irregardless of transaction size, religion, ethnicity, geography, etc) and strictly utilise the collateral in the manner that it is intended to be used (defined by the transparent

code base which defines these conditions). The fungible collateral has a public market price so that customers understand the exact market value of collateral being used (unlike a pawn broker).

In short, the smart contract allows collateralised lending to occur on a basis that is extremely transparent, well defined, and is based on the true market value of the asset in question to ensure a fair outcome to both borrower and lender.

The key risks of a smart contract application are technical vulnerabilities or economic model vulnerability. Protocols can be hardened through audits, bug bounties, governance discussion, performance monitoring and continued testing of parameters. Through taking such actions, the largest and most reputable collateralised lending protocols have proven to have limited vulnerabilities that have been minor in nature.

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?

Without quantifying data from the opaque pawn broking industry, I can inform you that during the recent crypto market drawdown, when several centralised lending/borrowing desks experienced significant losses and ultimately declared bankruptcy (Blockfi, Voyager, Celsius, Genesis), no reputable decentralised smart contract lending application failed. In fact, troubled asset managers repaid decentralised lending desks to meet the immutable and programmatically binding requirements in order to access their collateral before declaring bankruptcy.

No lender of crypto assets utilising the decentralised protocols AAVE and Compound experienced loss of asset during 2022.

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?

The primary risk in using a centralised crypto asset exchange is counterparty risk. Given the limited regulatory requirements of exchanges to date, this has led to several instances where customers have experienced large losses (FTX[8], Quadriga[9], Mt. Gox[10], Cryptopia[11], MyCryptoWallet[12], Thodex[13]).

[8] Embattled crypto exchange FTX files for bankruptcy
[9] Controversial QuadrigaCX cryptocurrency exchange placed in bankruptcy
[10] Mt Gox abandons rebuilding plans and files for liquidation
[11] Update for Cryptopia account holders 27 May 2019
[12] MyCryptoWallet collapses, appoints liquidators
[13] Digital Era Digital Risks: Tha case study of Turkish Crypto Currencies market

For a customer of a reputable AMM, the key advantage is that they are able to retain custody of their assets, and not rely on the solvency of the exchange or counterparty conducting the transaction.

Liquidity providers of AMMs have additional risks as their assets become controlled by the protocol at the time of liquidity provision. Whilst always maintaining a claim to those assets, should the protocol fall subject to a technical vulnerability, user assets can be stolen.

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

Decline to answer but there is data available.