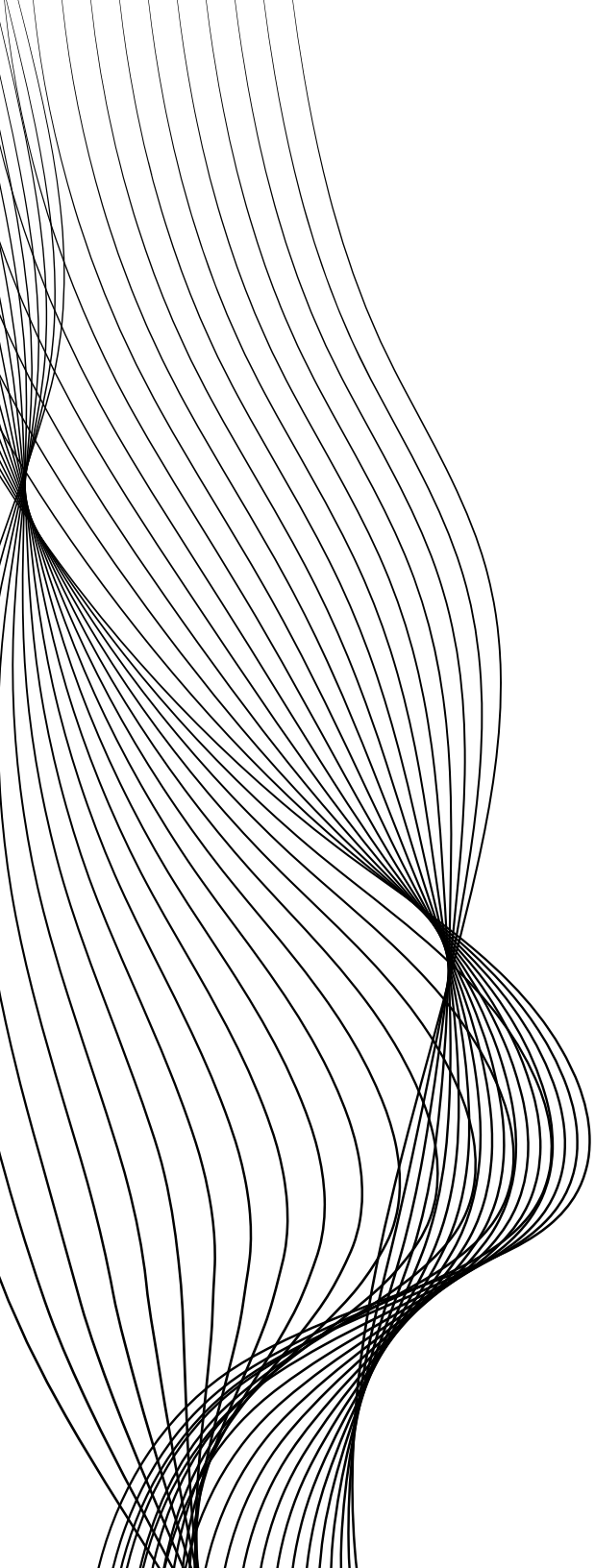
Submission

The Treasury

Token Mapping Consultation

DOXED CAPITAL

FEBRUARY 2023



Att: Director

Crypto Policy Unit

Financial System Division

The Treasury

Langton Crescent

PARKES ACT 260

As blockchain & crypto market analysts, we would like to participate in Treasury's Token Mapping Consultation.

We are providing this information to help nurture and support the growth of a vibrant Australian blockchain industry.

Table of Contents

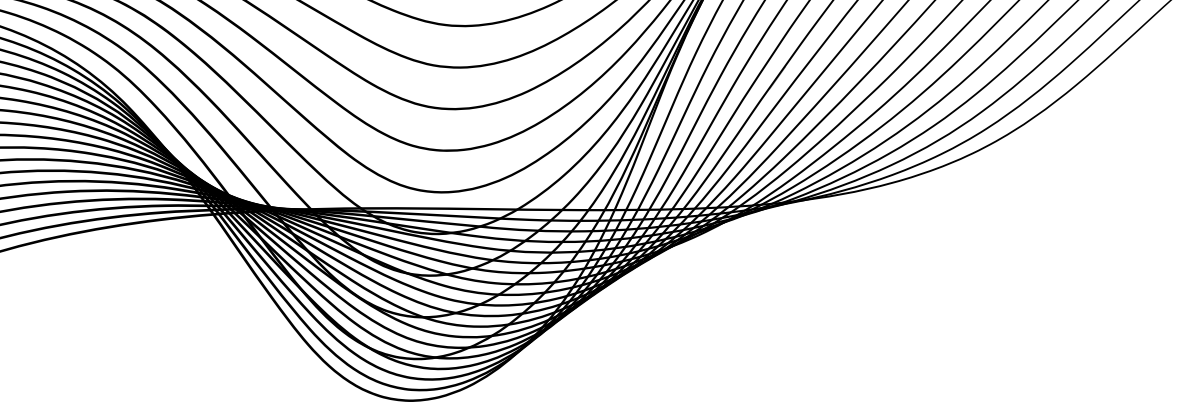
Q1) What do you think the role of Government should be in the regulation of the crypto ecosystem?

Our Response:

We feel that the role of government in the crypto ecosystem could be as follows:

Safety

Educate and inform the public about the risks of investing in digital tokens that are still an evolving class of assets, prone to regular demand and supply side shocks and also technical issues.



Opportunity

Communicate the long-term opportunities of blockchain and crypto as valid areas of employment and entrepreneurship that contribute to Australian economic growth.

Trust

Enact law and policy to help stabilise the crypto ecosystem by punishing bad actors, rewarding good behaviour, regulating crypto service providers and fostering a culture of investment in blockchain and crypto startups.

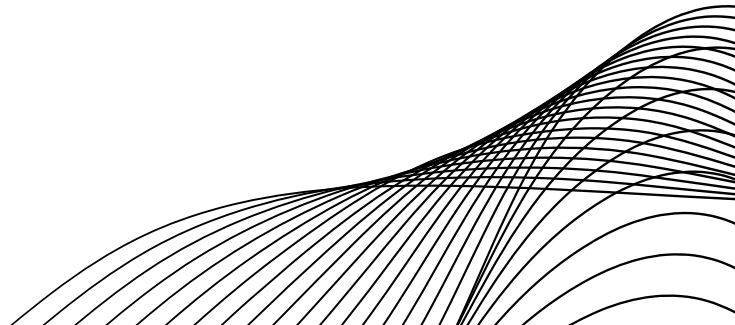
Guide

Guide thought-leadership about blockchain enabled decentralisation of financial services in ways that avoid eroding protection for consumers.

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

Our Response:

Establishing crypto safeguards via regulation is essential to the long-term viability of the blockchain and crypto industry. Regulation, could be informed by built-for-purpose governance structures that are established to meet this need and provide advice to government following extensive industry consultation.



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?

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?

Our Response:

A. Smart contracts may be written, audited and appropriately insured for the amount of funds that are being transacted. Unfortunately, in the majority of cases this is not occurring, leading to harms when smart contracts fail or are attacked by unscrupulous people.

We feel that layer 1 blockchains could be the most appropriate place to commence consultation about smart contract regulation because:

- they are large organisations who are easy to identify in contrast to their users
- they receive fees (gas) from smart contracts in return for processing transactions on their blockchain

For proof of stake blockchains, the relevant consultation group for regulators are validators, who are in effect, the blockchain's governance body and are confirming each transaction and receiving the gas payments.

For proof of work blockchains, the relevant consultation group are miners, who receive rewards by processing transactions on chain.

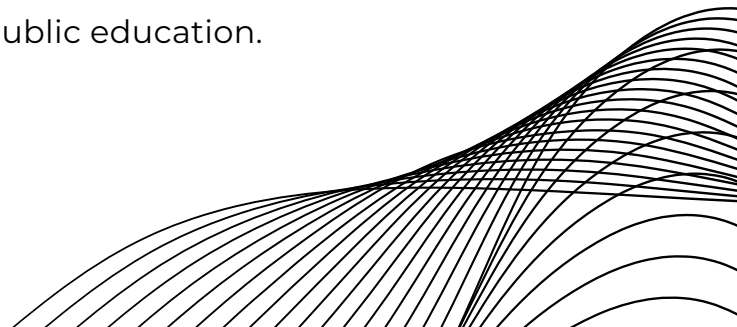
Whilst we believe that blockchain validators and miners are a common-sense "commencement point" for consultation, we do not feel that they should be compelled to carry the full burden of regulatory advice-giving, that could also be shared with builders and coders who are writing smart contracts to the blockchain.

B. Unlicensed, decentralised crypto exchanges can provide opportunities for the listing of scam tokens by unscrupulous individuals who hide in the anonymity that is possible.

   In contrast, centralised crypto exchanges come in a variety of types, ranging from scam exchanges to more reliable, licensed exchanges.

   A published system of crypto exchange safety ratings could help prevent consumers sending money to risky exchanges in the first place, before a token purchase occurs.

   In addition, a crypto exchange fact sheet that highlights the differences between licensed and unlicensed crypto exchanges could be a useful resource to aid public education.



Once a consumer has deposited funds with a licensed exchange and purchased crypto tokens on the spot market, there are still a number of loss-causing events that are possible including:

1. Project failure - the project founders decide to wind up the organisation.

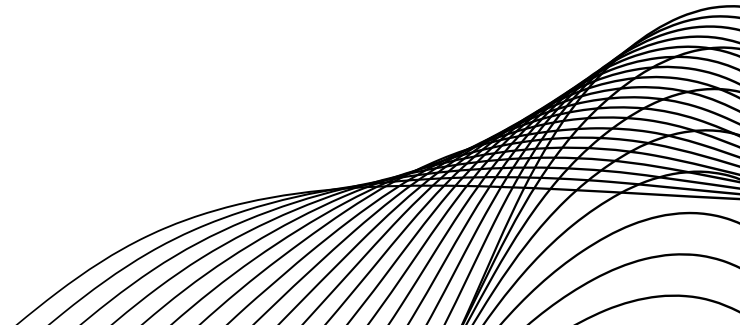
2. Project scam - the founders decide to mint and dump a large number of the project's native token.

3. Project hack - the project's smart contract is exploited by hackers who drain all the available liquidity.

4. Removal of trading pair - the exchange has decided it is no longer profitable to offer the trading pair, so it announces its removal.

Ideally, specific policy levers could be targeted at each one of these events, in ways that are workable for crypto exchanges to implement.

Such regulation, could be established via appropriate policy governance committees that include representation from crypto exchanges, layer 1 blockchains, traders, crypto startups, investors, policy analysts, legal professionals and digital scam investigators.



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.

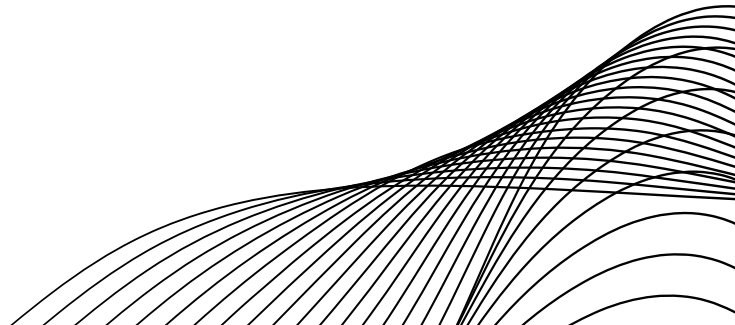
a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation?

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

Our Response:

A. Blockchain networks provide trustless technology for the publishing and control of public information that is required to be transparent.

B. The transparency of data stored on blockchains in the public domain is a major advantage that cryptographic technology has over private networks, making blockchain suitable for public data initiatives that place a high value on openness, access and trust.



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?

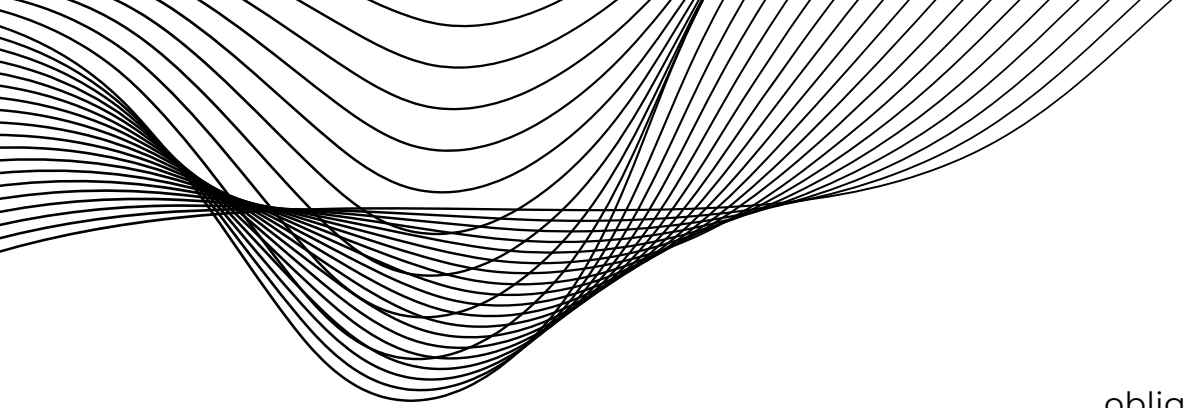
b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

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?

Our Response:

A. Grouping the diversity of digital asset activity into a smaller number of categories is useful to support the creation of high-level, strategic crypto policy and guiding principles to inform the overall approach to legislation and regulation of digital asset markets. Less so, when one wishes to establish precise regulation that applies to a given type of crypto asset or blockchain transaction.

B. In the quest for regulatory certainty, government could implement a bespoke taxonomy that uses the same names for digital asset and crypto activity that are used in the marketplace. Such an approach recognises that the customers of regulation are the people, and, that we are



obliged to meet them where they are, using their language. It is also likely that appropriate regulation, couched in terms used by the people and the industry will have higher levels of understanding, lower levels of ambiguity and a greater incidence of compliance.

C. We will pass on this question.

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.

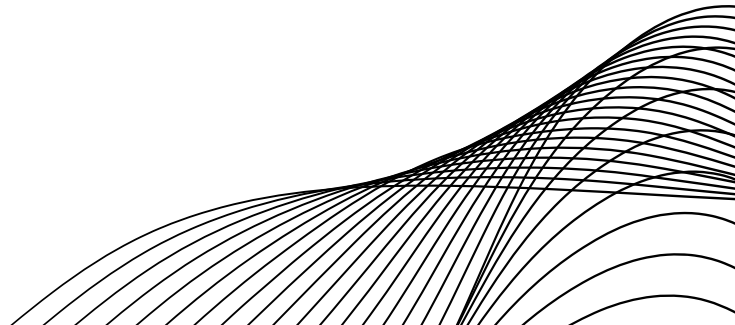
a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?

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?

Our Response:

A. The crypto term “wrapping” is used when we are making a given digital currency eg Bitcoin, available for transacting on an alternative blockchain, eg Ethereum. Such “wrapped Bitcoin” may be traded for its underlying value in the Ethereum ecosystem and later be unwrapped back into (normal) Bitcoin that exists on the Bitcoin network.

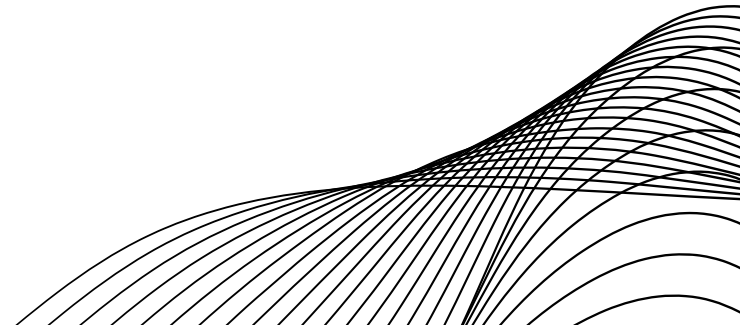
   In contrast, the “Tokenisation” of physical assets involves the issuing of tokens using a blockchain that represent an underlying physical asset.



These tokens could be issued using an NFT standard that allows for not only single assets to be bundled into an NFT but also multiple assets, further adding to the complexity of what is possible.

Alternatively, physical asset(s) could be tokenised as a fixed number of crypto tokens from a given blockchain smart contact. The total number of tokens issued multiplied by the price of the tokens, should accurately reflect the underlying market value of the physical assets being represented or tokenised.

B. We need to be clear about what we mean by “issuer of wrapped real-world assets”. For example, the person who owns the physical asset in the real world may not be the same person who mints and issues the asset-backed token via a digital wallet, as this function could be carried out by a service provider. The NFT or digital token(s) representing the physical asset(s) may then be placed on a marketplace for sale by a different person, again, also potentially as a service provider. Appropriate regulation could apply specific controls on each of these separate processes to ensure there are no loopholes or ambiguity in the seller’s burden of responsibility for the sale and redemption of physical asset-backed NFTs or tokens.



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?

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

Our Response:

A. Crypto asset service providers could provide links to crypto token information services such as Coingecko and CoinMarketCap that provide information about the tokenomics of crypto token projects, plus external website and social media links. Crypto service providers could include a disclaimer that indicates they bear no responsibility for the accuracy of crypto information provided by Coingecko or CoinMarketCap.

B. Leading crypto asset service providers could regularly publish informative articles and tutorials to help users better understand crypto assets. One example is Binance Academy.

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?

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

Our Response:

A. Most crypto assets are designed to have a transaction facility back into other crypto assets. The extent to which these transactions are possible depends on the availability of liquidity on both sides of the transaction. Without such liquidity, transactions are not possible and the holders of crypto assets can become economically marooned. In this sense, the liquidity provided by crypto market-makers, is what makes crypto a financial product.

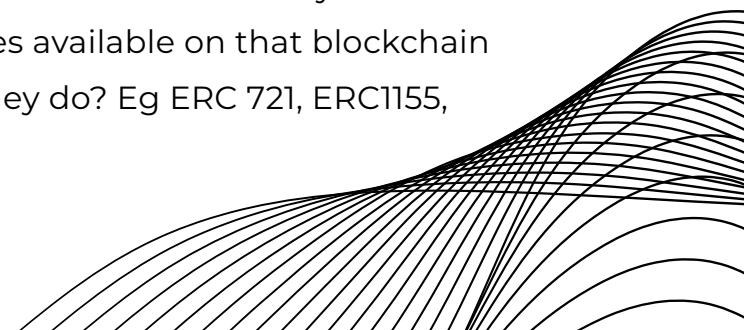
B. For the reasons mentioned above, we believe that crypto market-makers and liquidity providers should be defined as financial service providers.

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?

Our Response:

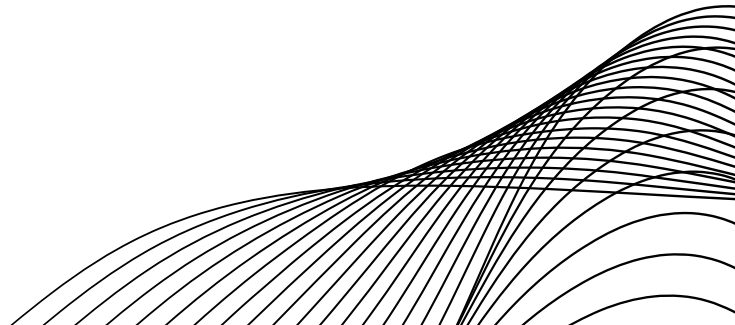
In deciding which blockchains should be able to host wrapped or tokenised real world assets, regulators could consider:

1. Liquidity - is there adequate invested liquidity in the native token of the blockchain to facilitate appropriately sized real-estate transactions without having large market or price impact?
2. ESG - is the blockchain validated by an energy efficient proof of stake network of validators? Or if a proof of work network, are its miners predominantly using renewable energy to carry out their mining activity?
3. Token diversity - what is the diversity of NFT and other token types available on that blockchain and what can they do? Eg ERC 721, ERC1155, ERC20.



We will pass on this question

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?

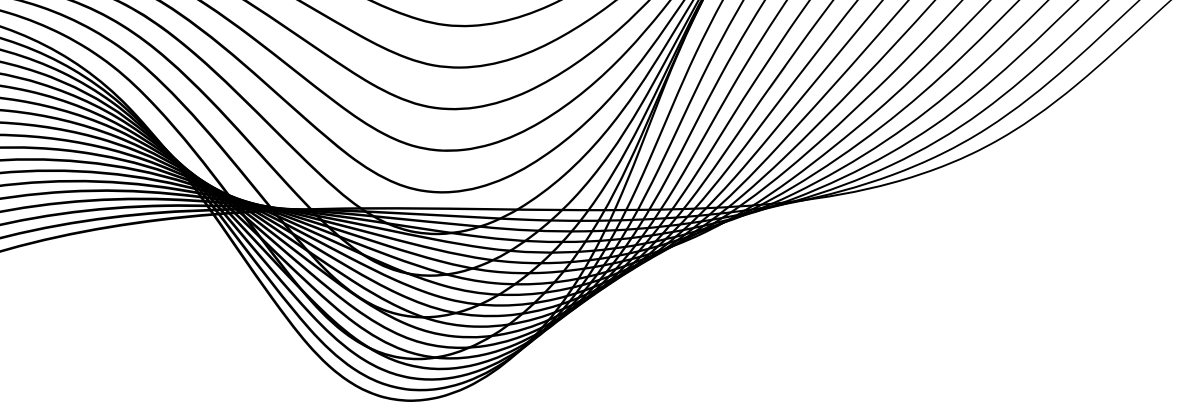


Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

Our Response:

Social media platforms and other mass-market advertising organisations could be required to conduct a due diligence process before approving a crypto advertisement.
Some of the major platforms are doing this already via robot and AI filtering of ad messages before they are allowed to go live.

The most harmful types of scam advertisements occur when hackers find a backdoor into the password and delegation system of the social media platform itself and then sell these keys to other scammers who pay to use them for profit.



Once scammers have the password backdoor, they hijack the social media account of a major influencer (with a large audience) and then post their too-good-to be true offer, leading to the draining of funds from followers who mistakenly believe the offer is genuine and endorsed by the influencer.

In the interests of combatting such issues, the UK are implementing a system of “authorised persons” licensed by the FCA who are allowed to place crypto ads.

The new UK FCA crypto advertising rules are a step in the right direction, however without significant resources dedicated towards enforcement, they may not impact the large amount of subtle crypto advertising that occurs via social medial influencers. Influencers, that may be compensated by crypto projects in any number of ways. For this reason, regulators may find it advantageous, to consider the creation of specific rules that address crypto infuencer advertising.

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

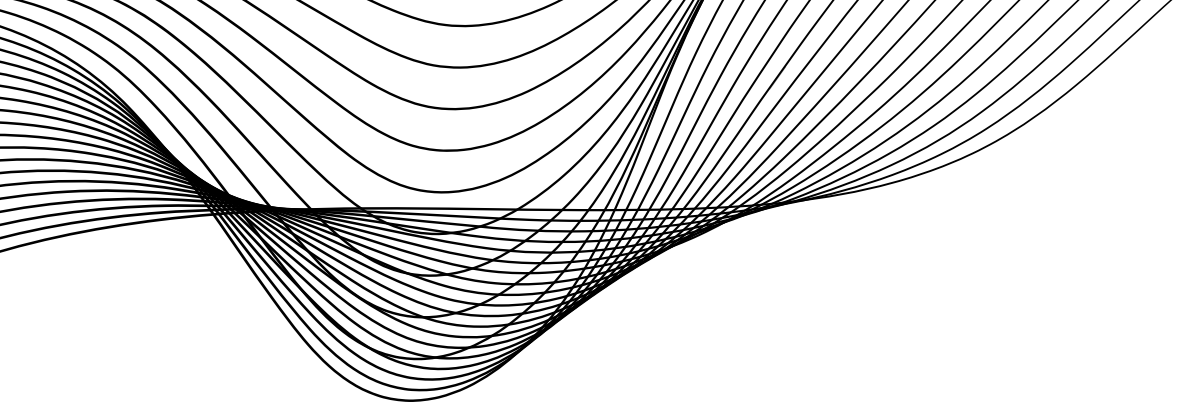
a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

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

Our Response:

A. Different blockchains require a range of programming languages to code smart contracts including Solidity, Rust, Javascript, C++, Web Assembly, Cadence, Golang, Python and others. Programmers who wish to code regulatory compliant smart contracts could be made aware of certain (to be designed) smart contract standards that permit contract owners to carry out the following operations when required:

- pause or commence contract operation
- kyc users
- generate reports about smart contract activity ie transaction size, type, destination
- publish or un-publish a contract
- interact with regulatory smart contracts



In the first instance, such compliant smart contracts could be configured to generate reports for a regulator to review. But, in the fullness of time, we might expect regulators to develop their own smart contracts that are able to interact with other contracts, extracting the data and information they require for compliance.

B. Most blockchains do not require KYC in order to publish a smart contract, as such information collection may be seen as going against the philosophy of decentralisation and resistance from censorship.

   Nonetheless, smart contracts do require a digital wallet address in order to be published.

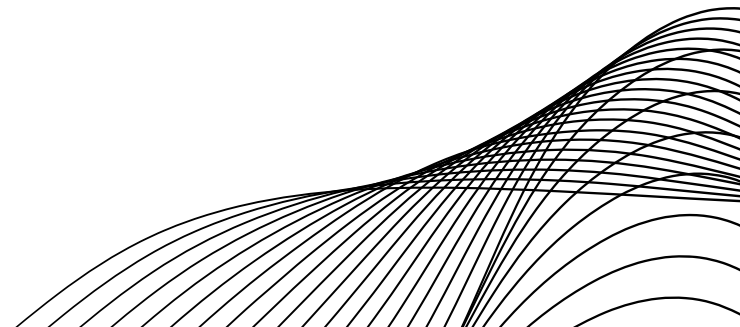
Part of the problem regulators presently have with decentralised smart contracts, is that the wallet identity for the majority of people using this ecosystem is unknown, making it difficult to sanction bad actors.

It is true, that regulators could introduce legislation to make owning a decentralised wallet illegal, but such a measure would stifle and sideline the benefits of crypto and blockchain development for that country.

A more workable policy approach could be to incentivise people to register their decentralised wallets on a centralised database owned by the government.

Helpfully, there are a growing range of decentralised technologies that could make the process of wallet-owner identification somewhat easier for regulators.

For example, Ethereum Name Service (ENS) allows a person to register a name for their decentralised wallet address eg “sandysmith.eth”. Such wallet naming services are also being made available on other blockchains.



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).

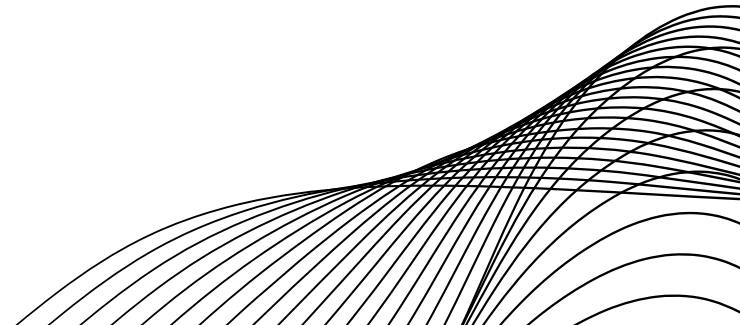
a) What are the key risk differences between smart-contract and conventional pawn-broker lending?

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?

Our Response:

A. A smart contract holds all the loan collateral “on chain” and will automatically liquidate the collateral when certain price or repayment conditions are met or not met. In contrast, a person borrowing from a pawn shop who risks defaulting on their payment can attempt to renegotiate terms with the lender to avoid liquidation.

B. We’re not aware of any, but it sounds like a good research question.



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?

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

Our Response:

A. AMM's function as online, robot markets that allow for the automatic exchange of crypto tokens, subject to their being sufficient liquidity available. There is no customer support. AMM's have their place by allowing for the formation of markets between far-flung groups of buyers and sellers that would otherwise not appear and participate. AMM's also are positioned at the maximum end of the risk scale, with nobody to turn to when things go wrong and no administrator policing bad actors who attempt to subvert AMM's into actions they were not designed for.

B. Please refer to the following study that collected data about the high number of scam coins published on the well-known AMM - Uniswap. In our experience, the riskiest, scam-filled coins and tokens are published to AMM's because there is no barrier to entry for the publisher. Still, there are also a number of legitimate coins listing on AMM's who try and grow enough following and momentum to attract a CEX listing.

It is also worth noting there are a small number of scam CEX's, whom allow deposits and trading but block withdrawals. Therefore, users should not assume, if they are dealing with a CEX, that they will automatically be safe, as not all CEX's are created and managed equally. Generally speaking, using a licensed exchange is safer, but consumers should still be made aware that crypto in any shape or form is a volatile, high-risk activity.