Australian Government
The Treasury

Token Mapping

Consultation paper

February 2023

treasury.gov.au

- Point needs to be clarified or further input.
- Missing points referring to other legislation – Gibraltar/MiCA etc.

CONTENTS

Consultation Process 1
Request for feedback and comments 1
Preliminaries 2

Foreword 3

A. Background 7
Introduction 7
Purpose of token mapping 7

B. Token mapping: terminology and concepts 11
Essential concepts 11
Mapping the crypto ecosystem 15

C. Intermediated token systems 20
Crypto asset services 20
Intermediated crypto assets 22
Regulatory and policy issues 24

D. Public token systems 28
Network tokens 28
Public smart contracts 31
Regulatory and policy issues 34

Conclusion 36

Annexure 1. Legal and regulatory framework 37

Annexure 2. Public crypto networks 43

Annexure 3. Smart contracts 46

Annexure 4. List of consultation questions 52

Annexure 5. Glossary 60

Consultation Process

Request for feedback and comments

The purpose of this paper is to seek feedback on the consultation questions contained within. Submissions may be lodged electronically or by post. Electronic lodgement via email to crypto@treasury.gov.au is preferred. For accessibility reasons, please submit responses sent via email in PDF format.

Publication of submissions and confidentiality

All information (including name and address details) contained in submissions may be made available to the public on the Treasury website unless you indicate that you would like all or part of your submission to remain in confidence. Automatically generated confidentiality statements in emails are not sufficient for this purpose.

If you would like only part of your submission to remain confidential, please provide this information clearly marked as such in a separate attachment. Legal requirements, such as those imposed by the *Freedom of Information Act 1982,* may affect the confidentiality of your submission.

Treasury will consult broadly with individuals and with representatives from industry, consumer groups, and other interested parties. This may involve conducting targeted roundtables and other consultation with interested stakeholders on specific issues to collect more information or to seek further views.

Closing date for submissions: 03 March 2023

Email	crypto@treasury.gov.au
Mail	Director – Crypto Policy Unit Financial System Division The Treasury Langton Crescent PARKES ACT 2600
Enquiries	Enquiries can be initially directed to Director – Crypto Policy Unit
Phone	02 6263 2111

Preliminaries

Generally, Treasury aims to provide policy advice that is technologically neutral. However, technical concepts are discussed as a critical part of the token mapping exercise.

The paper does not address all the risks of investing in crypto assets. It takes a technical approach in describing the crypto ecosystem and a legal approach in mapping the ecosystem against specific portions of the financial services regulatory framework.

A complete overview of the crypto ecosystem is beyond the scope of this paper. The paper relies on real examples to explain relevant concepts. Treasury has not assessed the crypto assets or crypto asset services examples used in this paper for their legitimacy, or investment and technological merits.

The principles outlined in this paper have not received Government approval and are not yet law. As a consequence, this paper is merely a guide as to how the principles might operate. Nothing in this paper is legal advice.

Foreword

The government is committed to improving the way Australia's regulatory system manages crypto assets – to provide greater protections for consumers and keep up with technological developments. This paper represents a foundational step in the Government's multi-stage reform agenda that will implement appropriate regulatory settings and support innovation.

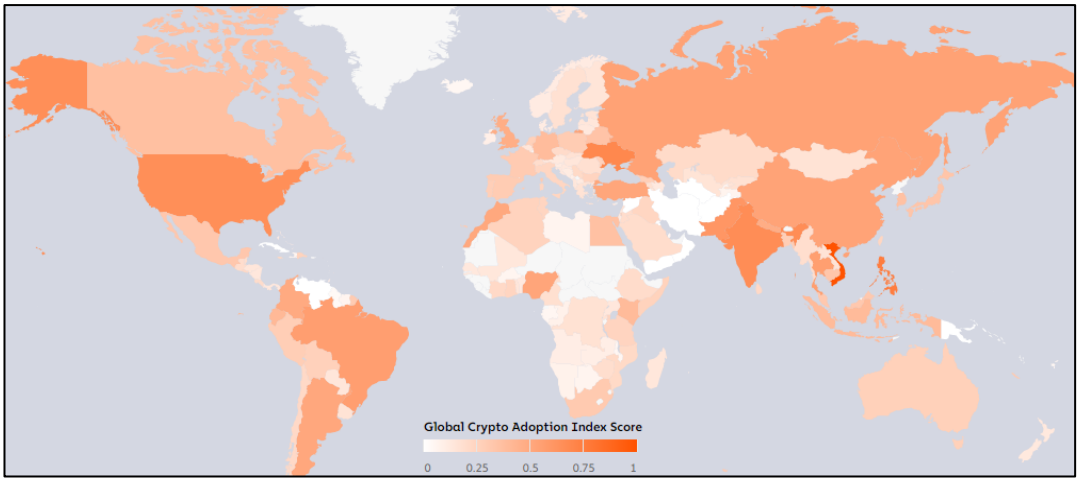
Token mapping plays a critical role in understanding the crypto ecosystem and ensuring a consistent and fair approach to the regulation of crypto assets in Australia. Primarily, this paper explores where existing regulation applies and helps set the path for future reforms.

Increased mainstream interest

Over the past decade, there has been increased mainstream interest from both financial markets and consumers in the crypto ecosystem. Over 1 million Australians are expected to include crypto assets on their tax returns in FY 2022. This trend has created emerging risks and opportunities.

According to Chainalysis' crypto adoption index, Australia ranks 40th globally for crypto adoption, with retail transactions at centralised exchanges also ranking 40th globally when measured by purchasing power parity per capita (see **Figure 1**).[1]

Figure 1: Global crypto adoption index



Source: Chainalysis September 2022

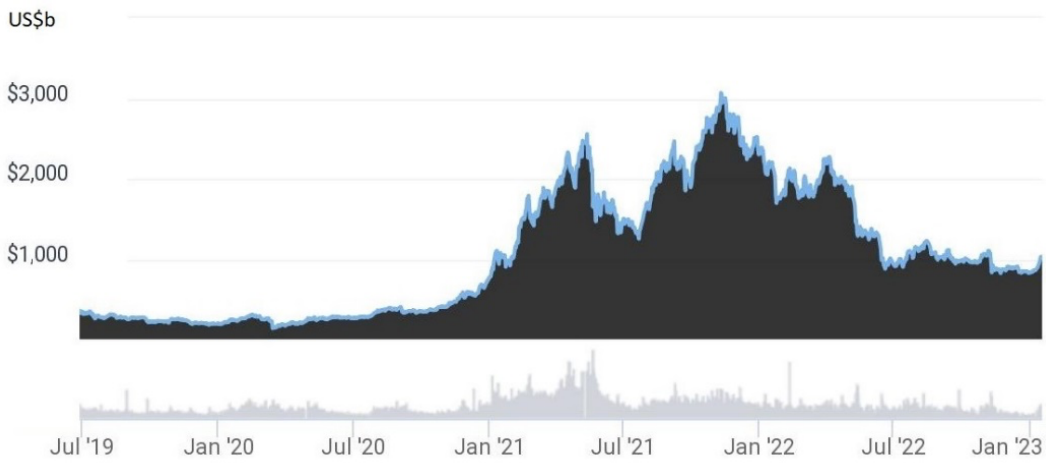
From global market capitalisation highs of US$3.0 trillion (AU$4.1 trillion) in November 2021, crypto asset markets have lost around 63 per cent of their value and are now valued at US$1.0 trillion (AU$1.5 trillion).[2] The turbulence in crypto asset markets over the past year highlights some of the risks. Since August 2022, crypto asset markets have experienced substantial volatility. This fall has been exacerbated by high profile failures of crypto projects and organisations (see **Chart 1**).

This volatility, combined with the increased exposure of Australian business and consumers to the performance of crypto assets, raises the risk that losses in this sphere could eventually feed through to impact the broader economy.

1 Chainalysis, Geography of Crypto *2022*, 14 September 2022.

2 CoinGecko, *Global Cryptocurrency Market Cap Charts*, as at 18 January 2023. Converted from USD to AUD using xe.com.

Chart 1: Crypto asset market capitalisation (2019 – present)



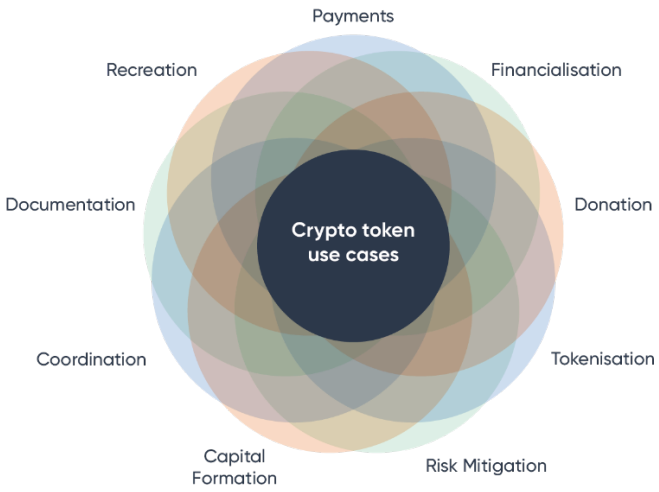
Source: CoinGecko

The technical and economic complexity, open and permissionless nature, and breadth of possible applications for 'crypto networks'[3] raise questions about how existing regulatory frameworks apply to the crypto ecosystem. This is particularly important where the crypto ecosystem intersects with the financial system.

The crypto ecosystem

The crypto ecosystem is not a homogenous industry or sector. Crypto networks are used by governments, businesses, non-profits, and individuals across sectors such as computer gaming, media and communications, logistics, gambling, marketing, and traditional finance. Similarly, 'crypto assets'[4] are not a homogenous asset class. They involve a vast range of different token types representing a wide variety of things, including communications, items in computer games, club memberships, bets, and legal entitlements to real-world assets, goods, and services (see **Figure 2**).

Figure 2: Crypto token use cases



3 The term 'crypto network' is used in this paper to refer to the various types of systems used to create and host crypto tokens. It has a similar but broader meaning than 'distributed ledger technology' (DLT). See **Part B** under 'Essential Concepts'.

4 The distinction between crypto *tokens* and crypto *assets* is described in **Part B**.

Risks

While the industry continues to develop and expand, crypto assets are still commonly associated with speculative trading, posing significant risks. Crypto products can be technically complex, highly price volatile, and difficult to custody safely. There are three key risks that need to be considered: (i) potential financial losses to consumers from engaging in the crypto ecosystem; (ii) potential financial risk to traditional firms engaging with the crypto ecosystem; and (iii) potential financial risk from the mainstream adoption of novel products that may turn out to be riskier than their traditional counterparts.

Consumer harm

Research by the UK Financial Conduct Authority found that in 2021 the most common reason for consumers buying crypto assets was '*as a gamble to make or lose money*'.[5] However, the research suggested that, year-on-year, it was becoming increasingly common for consumers to see crypto assets as an alternative or complement to mainstream investments.

In 2022, the significant price declines in crypto assets brought to light unsustainable business models used by some crypto ecosystem intermediaries. Liquidity mismatches, asset rehypothecation, and high leverage contributed to the collapse of several major crypto intermediaries, such as FTX. These intermediated elements of the crypto ecosystem do not adopt the transparency typically associated with crypto networks. Accordingly, consumers could not have been aware of these issues.

Customers of the collapsed businesses have lost billions of dollars. Some of the impacted customers may have been misled into believing their crypto assets were not subject to the control or management of any intermediary.[6] Many had purchased crypto assets that had no identifiable uses beyond speculation, or that had complex purposes they did not understand.

Scams also present a significant challenge. Common scams (including dating and romance scams, fake charity scams, investment scams, threats, and extortion scams)[7] may involve a request for transfers of crypto assets in place of requesting cash, bank transfers or gift cards. Scams within the crypto ecosystem may involve fake crypto assets, fake promises, or smart contracts designed with a 'back door' enabling the creator to steal (i.e. 'rug pulls').

In 2021, illicit use of crypto tokens globally was approximately US$14 billion, representing approximately 0.15 per cent of total legitimate crypto asset transactions.[8] The largest growth areas for illicit activity were scams and stolen tokens (US$7.8 billion). It can be difficult for some consumers to identify crypto scams or scams involving crypto assets. The online, fast-moving, and cross-jurisdictional environment also limits the capacity of regulators to interrupt and take enforcement action against perpetrators of scams.[9]

---

5 The next three most common reasons were: (ii) 'as part of a wider investment portfolio'; (iii) 'instead of buying shares or other financial instruments'; and (iv) 'as part of my long-term savings plan e.g. pension' – in that order. (See Financial Conduct Authority, 'Research Note: Crypto asset consumer research 2021', 17 June 2021).

6 Organisation for Economic Co-operation and Development (OECD), 'Lessons from the crypto winter: DeFi versus CeFi', OECD Business and Finance Policy Papers, 2022.

7 See ACCC, Types of Scams, SCAMWATCH website (n.d).

8 For the definition of 'illicit' activities used in these figures, see Chainalysis, 'The 2022 Crypto Crime Report: Original Data and Research into Cryptocurrency-Based Crime' (February 2022).

9 See ASIC, Crypto Scams, Moneysmart website (n.d.)

Financial stability

As the crypto ecosystem grows and attracts more investment, crypto assets become more intertwined with traditional financial markets. Recent years have seen a steady increase in the number of funds holding crypto assets on their balance sheets and the introduction of exchange traded funds (ETFs) tracking the value of crypto assets. In the future, this could pose additional risk to the financial system if linkages with traditional financial market become significant.[10]

Opportunities

Australia is already home to a thriving community of crypto ecosystem businesses, including network infrastructure providers, code auditors, trading platforms, online gaming companies, and software engineers. If the crypto ecosystem matures and develops, it could open significant new opportunities for businesses and consumers alike, creating jobs and fostering innovation.

The crypto ecosystem also has the potential to help improve competition in the technology and other sectors, which would carry broader benefits for the Australian economy. Australian businesses can take advantage of the technological advancements to improve their operations, create new opportunities for growth, build efficiencies into existing products, and explore new markets.

To capitalise on these opportunities and ensure consumer and business trust and confidence in the crypto ecosystem, regulation is required. This includes both clarifying where existing regulation applies, as well as ensuring that any additional regulation is appropriately robust, fit-for-purpose, and can keep pace with the rapidly evolving ecosystem.

International approaches to crypto ecosystem regulation

Globally, the regulatory frameworks for the crypto ecosystem are being actively considered with different approaches emerging. Some jurisdictions (e.g. Japan, Singapore) have started to modernise existing legislation. Other jurisdictions (e.g. European Union) have opted to draft crypto-specific legislation. Policy responses range from bans (e.g. China, Iraq) to government entities experimenting with issuing crypto tokens bonds (Hong Kong), announcing intentions to become crypto hubs (UK, Singapore), and establishing national crypto asset exchanges (Indonesia).

International standard setting bodies are monitoring developments closely and working to identify key elements of an effective policy framework.[11] Robust macro financial policies, sound legal and regulatory frameworks, as well as effective international coordination, are all being identified as key building blocks.[12]

10 Reserve Bank of Australia (RBA), 'Financial Stability Review', October 2022

11 Financial Stability Board (FSB), 'Regulation, Supervision and Oversight of Crypto-Asset Activities and Markets: Consultative Report', 11 October 2022.

12 International Monetary Fund (IMF), 'Some Key Elements of Crypto Regulation', 9 December 2022.

A. Background

Introduction

1. On 22 August 2022, the Government announced 'token mapping' – a foundational step in the Government's multi-stage reform agenda that commits to developing appropriate regulatory settings for crypto ecosystem in Australia. Token mapping is essential to understanding the crypto ecosystem and its intersection with Australia's existing regulatory frameworks – in particular, the financial services framework.

2. The paper is structured as follows.

   Part A - sets out key background information about token mapping, including describing the purpose of token mapping, the existing regulatory context, and next steps.

   Part B - outlines the essential concepts required to understand the crypto ecosystem, describes the financial services regulatory perimeter in the context of the crypto ecosystem, and proposes a high-level crypto ecosystem taxonomy.

   Part C - describes how the existing financial services framework applies to a large part of the crypto ecosystem – where consumers rely conventionally structured intermediary businesses.

   Part D - describes how some elements of the crypto ecosystem challenge the assumptions underlying existing Australian regulatory frameworks.

   Part E - summarises the conclusions made in this paper and outlines next steps.

3. Stakeholder feedback is sought on the consultation questions set out at the end of each section of this paper (a complete list of consultation questions can be found at **Annexure 4**). Stakeholder feedback will inform a fact based, consumer conscious and innovation friendly approach to policy development. Submissions received will help in formulating a framework for understanding tokens that will inform future policy choices.

Purpose of token mapping

4. Token mapping is the process of identifying the key activities and functions of products in the crypto ecosystem and mapping them against existing regulatory frameworks. In a recent paper on options for addressing the risks in the crypto ecosystem, the Bank for International Settlements (**BIS**) described how regulating the crypto ecosystem would require this kind of token mapping process as a foundational step.[13]

5. The BIS paper describes how the crypto ecosystem regulation could use the same principles and tools that apply to the regulation of traditional products. It states that regulation could start from a *functional* approach that involves: (i) identifying the key economic *functions* performed by crypto activities; and (ii) mapping those activities to those performed in traditional finance.

13 Aquilina et al., 'Addressing the risks in crypto: laying out the options', *Bank for International Settlements Bulletin*, 12 January 2023.

Why token mapping makes sense for Australia

6. The approach described in the BIS paper is attractive in the Australian regulatory context because it adopts core principles built into the existing financial services regulatory framework – specifically, technology neutrality and the functional approach to regulation.

7. Technology neutrality is a principle that has long applied to Australian regulatory frameworks. This is to ensure regulation stays fit for purpose as business models and technologies change. The importance of this concept in financial regulation was highlighted by the 1996 Wallis Inquiry and the 2014 Financial System Inquiry.[14]

8. Australia's functional approach to financial regulation largely gives effect to the policy adopted after the Wallis Inquiry that 'functionally-equivalent' products should be treated equivalently.[15] It was introduced to remove barriers to technological innovations and with the intention that it would be capable of flexible implementation.[16]

9. Australia differs from most other jurisdictions by adopting a broad *functional* definition of 'financial product' as part of defining the financial services regulatory perimeter (**functional perimeter**).[17] Other jurisdictions exhaustively list regulated products and may be guided by risk-based or activities-based approaches in updating those lists to include novel financial products.[18]

10. Australia's *functional perimeter* captures any 'facility'[19] through which, or through the acquisition of which, a person does one or more of: (a) makes a financial investment; (b) manages financial risk; and (c) makes non-cash payments (together, the '**general financial functions**').[20] The functional perimeter is supplemented by specific definitions of financial products, which are intended to both: (i) provide guidance on the functional perimeter; (ii) add additional products that do not fall within the general financial functions.

Role of Government in regulation

11. Governments play an important role in facilitating healthy economic and social environments for interactions between businesses and their customers. This includes identifying the appropriate level and form of intervention in free and competitive markets. Government intervention in markets for products and services has traditionally taken the form of regulation that creates: (i) rules to ensure the markets are fair, efficient, and competitive; (ii) standards to ensure the safety and quality of the products and services; or (iii) measures that encourage or discourage certain activities.[21]

---

14 Australian Law Reform Commission (ALRC), 'Background Paper FSL7 Legislative Framework For Corporations and Financial Services Regulation: New Business Models, Technologies, and Practice', 2022.

15 A Godwin, 'Crypto Assets and the Challenges for Regulatory Design', *TechREG Chronicle* (*May* 2022).

16 Minister for Financial Services and Regulation, Second Reading Speech, Financial Services Reform Bill 2001, 5 April 2001.

17 Australian Law Reform Commission, 'Financial Services Legislation: Interim Report A', 2021, pg 287 [7.66].

18 Godwin, 'Crypto Assets and the Challenges for Regulatory Design', *TechREG Chronicle* (May 2022), pg 6; and ALRC, 'Interim Report A', 2021, [7.65].

19 The definition of 'facility' is broad. It includes any intangible property and a term of any arrangement (whether or not the term is formal, written, implied or required by law, or legally enforceable). Two or more arrangements may be taken to constitute a single arrangement (see **Annexure 1**).

20 **Annexure 1** contains further detail on the functional definition of a 'financial product' (including a description of the general financial functions).

21 S Wallis et al, 'Financial System Inquiry (1996) Final Report', Australian Government, 1997 [Chapter 5].

12. Some implementations of financial services regulation seek to construct specific guardrails to prevent retail consumers from being exposed to risky products (e.g. design and distribution obligations and sophisticated investor laws). An absence of regulation can also result in potential benefits of new products and services not being realised due to a lack of consumer trust in the new systems, which in turn can discourage investment from innovators.

How token mapping will inform future policy development

13. Token mapping introduces important elements of the crypto ecosystem and the existing financial services regulatory landscape. However, crypto networks can be complex systems.[22] This paper aims to explain key concepts in simple terms for a broad audience.

14. Token mapping is a key first step to planned and future crypto ecosystem initiatives. In describing the breath of the ecosystem and the emerging innovations and opportunities, and in applying the same principles and regulatory tools that apply to the regulation of traditional products, a token mapping-based strategy can:

    (a) ensure consistency in regulating activities (i.e. be technology neutral)

    (b) facilitate existing policy goals (i.e. not require the wholesale creation and adoption of a standalone policy that may overlap or conflict with existing policy)

    (c) allow responsible actors to innovate with appropriate regulatory oversight.

15. Submissions received in response to this paper will initially inform future policy choices on licensing and custody and potential amendments of the existing financial services frameworks.

Future policy – next steps

16. After token mapping, licensing and custody reforms are the logical next step for crypto reforms in Australia. The identification of appropriate obligations and operational standards for crypto asset service providers and how they safe-keep assets for customers is a key step for consumer protection; ensuring consumers do not lose assets to avoidable business failure or misuse of assets by the provider.

17. The Government will release a consultation paper proposing a licensing and custody framework for crypto asset service providers in mid-2023 to allow for sufficient consultation prior to the introduction of legislation. The paper will reflect ongoing work and consultation in this area and leverage the findings from the token mapping exercise. The responses to the following questions will help inform the general direction of future policy and potential consumer protections.

22 S Voshmgir and M Zargham, 'Foundations of Cryptoeconomic Systems', (2020), Institute for Cryptoeconomics and Interdisciplinary Research, WU Vienna University of Economics and Business.

Consultation questions

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

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

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 exhanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?

B. Token mapping: terminology and concepts

18. Crypto assets are not excluded or 'carved out' from Australia's financial services regulatory framework. Any product (including a crypto asset) will be a financial product if it falls within the function perimeter or meets one of the specific definitions of financial product – regardless of its technological underpinnings.

19. A large portion of the crypto ecosystem today is either: (i) businesses offering products that relate to crypto assets; or (ii) businesses creating crypto assets that relate to existing non-crypto products. Mapping these products against the functional perimeter shows that:

    (a) some products have clear financial functions (e.g. crypto asset services offering crypto derivative products, or crypto assets 'backed' by existing financial products); and

    (b) some products have clear non-financial functions (e.g. crypto tokens used for document provenance, digital identity, general record keeping, data storage, and crypto assets used in event ticketing).

20. However, there are some elements the crypto ecosystem that may not fit the existing regulatory models. These elements involve free open-source software that can be used by parties who are unknown to each other to form transactional relationships in the absence of intermediaries or agents. These relationships are represented by crypto tokens created by the parties themselves. These crypto tokens can have functions that are ensured in the absence of promises. In some cases, the functions are clearly financial. These parts of the ecosystem are considered in Part D.

21. A key innovation of public crypto networks is that they can be used as neutral, independent, and immutable infrastructure for high value activities between unknown parties.[23] However, the absence of promises, intermediaries, and agents causes some issues in financial regulation. The Wallis Inquiry noted that "*The purposes of financial regulations are to ensure at least that financial promises are understood and, in their more intense form, that they are met.*" The final report of the Wallis Inquiry explained that financial regulation targets the performance of intermediaries, agents, and financial markets in meeting the promises underlying financial contracts.[24]

22. The financial regulatory framework that was created following the Wallis Inquiry created boundaries, obligations, protections, and supervisory powers that assume financial market risk is largely centred around the three concepts of promises, intermediaries, and agents. Accordingly, products that truly involve none of these three concepts may – without reforms and new regulatory approaches – be fundamentally incompatible with the existing financial services regulatory framework.

Essential concepts

23. There is currently no consensus – either in Australia or globally – on the meaning of key concepts in the crypto space. A single concept may have varied and conflicting meanings across industry, academia, and government institutions. This paper defines and outlines the key concepts of 'crypto networks', 'crypto tokens', and 'smart contracts', below.

---

23 F Schär, 'DeFi's Promise and Pitfalls', *International Monetary Fund: Finance and Development*, September 2022.

24 S Wallis et al, Financial System Inquiry (1996) Discussion Paper, Australian Government, 1996 [Chapter 4] and S Wallis et al, Financial System Inquiry (1996) Final Report, Australian Government, 1997 [Chapter 5].

24. An agreed understanding of these concepts between stakeholders and policymakers is the first step towards identifying: (i) the elements of the crypto ecosystem that fall inside and outside the existing regulatory perimeters; (ii) the key risks that are added or removed by products using crypto networks; (iii) the sensible regulatory targets for a future regulatory framework; and (iv) the legitimate technical criticism and anticipated opportunities of the technology.

25. The following section seeks to describe key concepts in a way that strikes a balance between: (i) accuracy and precision; (ii) emerging international convention; and (iii) conflicting, outdated, or overly complex constructions. Footnotes are used throughout this section to provide further information on challenging topics and to assist stakeholders with their submissions.

Crypto networks

26. A **crypto network** is a distributed computer system capable of hosting crypto tokens. Crypto networks are the platforms on which crypto tokens and 'smart contracts' are recorded. Their primary function is to store information and process user instructions.

27. The description of 'crypto network' used in this paper is technology neutral, simple and broad.[25] It is intended to cover all the various data structures and technologies used for hosting crypto tokens, including well known DLTs such as blockchains.[26]

28. The two largest crypto networks (the Bitcoin and Ethereum networks) host close to 80 per cent of the entire market capitalisation of crypto assets.[27] They are 'public crypto networks' – each made of up of several thousand individual computers maintained by a globally distributed network of users.

Public crypto networks

29. A **public crypto network** aims to provide certain information security guarantees in a way that does not require a trusted third party to store and process data. They rely on public communication and data standards (i.e. protocols), which are typically maintained by an open group of volunteers (made up of individuals, academics, non-profits, and corporates) who contribute development resources, research, and funding.[28]

30. A public crypto network is established when a distributed group of individual computers begin communicating and processing information by following the agreed standards. If there are no restrictions on the computers that are *allowed* to join the network, it creates an open information processing system that cannot discriminate between users or use cases.[29] There are clear parallels between public crypto networks and the internet.[30]

---

25 It does not refer to the use of cryptography and distributed databases because those features are common across other distributed systems (e.g. cloud computing, the SWIFT network).

26 For example, blockchains (Bitcoin and Ethereum), directed acrylic graphs (Hedera and Fantom), state channels (Lightning), optimistic rollups (Arbitrum One and Optimism), zero knowledge rollups (zkSync and StarkNet), validium solutions (zkPorter and StarkEx).

27 BTC on the Bitcoin network (39 per cent), ETH on the Ethereum network (18 per cent), and smart contract tokens on the Ethereum network (20 per cent).

28 L Dashjr, 'Bitcoin Improvement Process, Revised' (BIP-2, 3 February 2016); and H Jameson, 'Ethereum Protocol Development Governance and Network Upgrade Coordination', Hudson Jameson website, 23 March 2020.

29 V Buterin, 'Credible Neutrality As A Guiding Principle', nakamoto.com website, 4 January 2020.

30 M Iansiti and K Lakhani, 'The Truth About Blockchain', Harvard Business Review (2017) 95(1), 118–127; and P De Filippi and A Wright, 'Blockchain and the Law: The Rule of Code' (Harvard University Press, 2018), pg 46.

31. Proponents of public crypto networks argue that they can be used to replace costly mechanisms of intermediation and legal enforcement with new forms of 'trustless trust'[31], 'confidence'[32], or 'information hardness'.[33] Technical critics argue, however, that the technology is a solution looking for a problem,[34] is not new or innovative,[35] requires too much transparency,[36] or still requires several layers of intermediaries.[37]

32. In any event, there are significant non-trivial engineering and cryptographic advancements needed for crypto networks to scale to a level of supporting mainstream adoption,[38] which may be years or decades away.[39] Most activities involving crypto assets currently occur through 'crypto asset services' (e.g. crypto asset exchanges, lending and borrowing services) – who are typically intermediaries providing services adjacent to crypto networks using conventional computing infrastructure.

Crypto tokens

33. A **crypto token** is a unit of digital information that can be '*exclusively used or controlled*' by a person – despite that person not controlling the host hardware where that token is recorded.[40] The concept of 'exclusive use and control' is a key distinguishing factor between crypto tokens and other digital records. It has been used in legal frameworks and considered in detail by peer jurisdictions.[41]

34. Another key distinction between crypto tokens and other record keeping devices is that the authenticity of a crypto token is established using a branch of mathematics known as 'cryptography'.[42] In contrast, the authenticity of a physical token (e.g. a casino chip or concert ticket) is established using their physical properties, and the authenticity of a conventional registry entry is established by a registrar.[43]

---

31 K Werbach, 'Trust, But Verify: Why the Blockchain Needs the Law', *Berkley Technology Law Journal*, 2017, 33.

32 P De Filippi, M mannan and W Reijers, 'Blockchain as a Confidence Machine', *Technology in Society*, 2020, 62.

33 J Stark, 'Atoms, Institutions, Blockchains', *Mirror*, 13 April 2022.

34 B Schneier, 'On the Dangers of Cryptocurrencies and the Uselessness of Blockchain', *Schneier on Security*, 24 June 2022.

35 D Rosenthal, 'EE380 Talk: Stanford Seminar – Can We Mitigate Cryptocurrencies' Externalities', *DSHR's Blog*, 2022.

36 Ben-Sasson et al, 'Scalable, Transparent, and Post-Quantum Secure Computational Integrity', *Cryptology ePrint*, 2018, 46.

37 M Marlinspike, 'My First Impressions of Web3', *Moxie,* 7 January 2022.

38 M Green, 'In Defense of Crypto(Currency)', *A Few Thoughts on Cryptographic Engineering,* 9 June 2022.

39 M Iansiti and K Lakhani, 'The Truth About Blockchain', Harvard Business Review (2017) 95(1), 118–127.

40 Existing definitions reference underlying technology (e.g. by referencing data on 'cryptographic, distributed databases' or specific data structures like blockchain). These definitions are often complex (in attempting to carve out technically similar systems) or overly simple (inadvertently capturing systems used for everyday purposes).

41 For a detailed consideration of the concept (and the alternative concept of 'rivalrous data') see Law Commission (UK), 'Digital Assets: Consultation paper', 2022. For an example of its use in legislation see Uniform Law Commission (US), 'Uniform Commercial Code Amendments 2022', Article 12, pg 229.

42 The purpose of 'cryptography' used in mainstream crypto networks is not to encrypt (i.e. hide) information. The entire transaction history of crypto networks such as the Bitcoin and Ethereum networks is available in clear text.

43 Microsoft Corporation, 'Tokenization: Establishing Digital Representations of Value', 2019.

Smart contracts

35. A **smart contract** is computer code that has been published to a crypto network's database. Smart contracts are not 'contracts' in a legal or plain English sense.[44] They are a fundamentally unique type of software that (on robust crypto networks) can be guaranteed to run in a predefined and deterministic manner without risk of intervention.[45] Smart contracts can be used to create self-service 'agents without agency' for a specific, pre-coded task – in a similar manner to vending machines.[46]

36. This paper uses three related terms when referring to smart contract-based products. These terms are briefly described in the box below and considered in more detail in **Annexure 3**.

Key 'smart contract' terms used in this paper

A **smart contract protocol** is a collection of smart contracts that can perform more complex and flexible functions than a single smart contract. An example of the flexibility is that they can be used to create software that is upgradable (allowing for iterative improvements and bug fixes) and controllable (allowing them to be used by intermediaries to provide services).[47] Smart contracts and smart contract protocols are the building blocks for 'smart contract applications'.

A **smart contract application** combines smart contracts with conventional technology (e.g. online data, computer servers, and websites/phone apps) to create a user-facing application. The same smart contract *protocol* can be adopted by multiple, unrelated smart contract *applications* (e.g. the Uniswap 'automated market maker'[48] is incorporated into wallet applications, exchange aggregators, investment platforms, and the product offerings of centralised exchanges).

A **smart contract token** is a crypto token that has been created using a smart contract. A vast majority of crypto tokens (by number) are smart contract tokens.[49] Any person with basic computer skills can create smart contract tokens using standardised, open-source software libraries.[50] Examples of existing smart contract tokens include most stablecoins, real-world asset tokens, non-fungible tokens (**NFTs**), governance tokens, and meme tokens.

---

44 However, they can be used as tools by contractual parties to facilitate the performance of an agreement (see M Giancaspro, 'The Consideration Myth About Smart Contracts', *(2020) 1(1) Australian National University Journal of Law and Technology 35.*

45 P De Filippi, C Wray, G Sileno, *'*Smart Contracts*'*, *Internet Policy Review*, 2021, 10(2).

46 They are like vending machines in that they are used to remove the need for certain business protocols (including standard form contracts, administrative routines, internal business controls, and compliance controls).

47 M Salehi, J Clark and M Mannan, 'Not so Immutable: Upgradeability of Smart Contracts on Ethereum', *arXiv*, 2022.

48 An automated market maker is a smart contract protocol that enables intermediary-less swaps between crypto tokens (see Uniswap v3)

49 There are various other ways to create non-network tokens on both general-purpose and cryptocurrency networks (see J Roth, F Schär and A Schöpfer, 'The Tokenization of Assets: Using Blockchains for Equity Crowdfunding' in Karen Wendt (eds), *Theories of Change*, Springer Nature, Switzerland, 2020).

50 Over three million smart contract tokens exist across the three most popular general-purpose crypto networks (see Ethereum (https://etherscan.io/tokens), Polygon (https://polygonscan.com/tokens), and BSC (https://bscscan.com/tokens)). Many of these have no transaction history after creation and may be explained by individuals completing 'token creation' tutorials.

Consultation questions

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?

Mapping the crypto ecosystem

Token mapping framework

37. This paper proposes a token mapping framework that relies on three key concepts: tokens, token systems and functions. These concepts are represented by the circle, square, and diamond graphic throughout the paper.

38. The token, token system, function framework can be used to consider the various products within the crypto ecosystem, and to assess them against the functional perimeter.

39. *Tokens* are physical or digital units of information that have a role in a *token system*. A token system is a collection of steps involved in performing a *function*. A function can be any benefit ensured or facilitated by the token system to the token holder.

40. It is important to identify the function because it is the key link to our existing financial services regulatory framework. The 'functional perimeter' of our regulatory framework captures facilities through which, or through the acquisition of which, a person undertakes 'general financial functions'. In the context of crypto, the relevant 'function' is the target of the assessment in the same way as any non-crypto product.

Components of the 'token, token system, function' framework

A **token** is a physical or digital unit of information. It could include:

(a) physical 'bearer-like' objects (e.g. the 'unique plastic disk and markings' that constitutes a casino chip)

(b) registry entries (e.g. the 'data' that constitutes the details of a shareholder in a company's shareholder register).

A **token system** is anything designed to ensure or facilitate a function. It could include:

(c) business protocols (e.g. a casino's internal procedure for facilitating casino chip redemptions)

(d) social protocols (e.g. the understanding between Monopoly game players on following the rules (including the meaning of each token))[51]

(e) physical protocols (e.g. the mechanisms that ensure access to a subway through a token operated turnstile).[52]

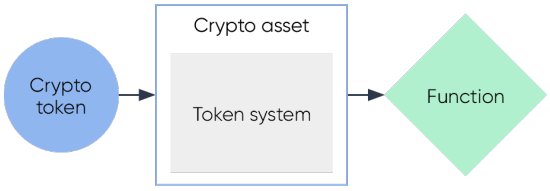
Token systems used in the provision of products and services are typically the procedures used to create and meet contractual obligations to customers. These contractual obligations may be overlayed with other legal rights and obligations, including those created by legislation and regulation.

A **function** can be any benefit ensured or facilitated by a token system (e.g. 'receiving money' (for a person redeeming a casino chip) or 'getting out of Monopoly jail' (for a player redeeming a get out of jail free card in a game of Monopoly)).

Applying the token mapping framework

41. The token mapping framework described above can be applied to 'crypto assets' and to products and services that use or rely on crypto assets.

42. A **crypto asset** is a 'token system' that is intrinsically linked to a *specific* crypto token. The intrinsic link means the term 'crypto asset' is effectively an umbrella term for a crypto token and each of the benefits provided by its token systems. An example of the 'token, token system, function' framework applied to a crypto asset is where ETH (crypto token) is accepted by the Ethereum network's 'fee market mechanism'[53] (token system) in exchange for using the Ethereum network (function).



43. The framework can also be applied to describe any product or service that uses or relies on an existing crypto asset in the performance of a function. In these cases, the relevant token system is not intrinsically linked to a particular crypto token. This would include 'crypto asset services' (defined in **Part C**) and public smart contracts (defined in **Part D**). An example of the 'token, token system, function' concept applied to a crypto asset service is where BTC (crypto token) is accepted as collateral as part of a lending arrangement (token system) in return for a loan of money (function).

---

51 Each 'player piece', card, note and house/hotel in a game of Monopoly is a token with different functions (see Microsoft Corporation, 'Tokenization: Establishing Digital Representations of Value', 2019, p5).

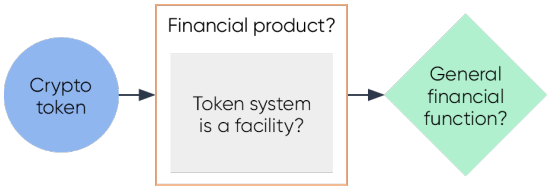
52 Token systems that use 'physical protocols' also include some vending machines and telephone boxes. For a description of a 'subway token' see New-York Historical Society, 'Remember The NYC Subway Token', *New-York Historical Society | Museum & Library,* 24 July 2014.

53 I.e. the mechanism used by crypto networks to regulate the supply and demand on network resources (see 'network tokens' in **Part D**).

Applying the 'functional perimeter'

44. As described above, Australia's *functional perimeter* is designed to be flexible, technology neutral, and innovation friendly. It captures any 'facility'[54] through which, or through the acquisition of which, a person does one or more of: (a) makes a financial investment; (b) manages financial risk; and (c) makes non-cash payments (together, the '**general financial functions**'). The definitions of each of the general financial functions is at **Annexure 1**.

45. Applying the functional perimeter is not a question of whether a *crypto token* meets the relevant definitions. It is a question of whether a *token system* does. This is a two-part question: (i) 'is the token system a *facility*?' and; (ii) 'is the facility one through which a person does any of the *general financial functions*?'. If the answer to *both* questions is 'yes', the *facility* is a financial product.



46. In addition to the functional perimeter, the financial services framework lists specific inclusions and exclusions of arrangements which are financial products. The inclusions are intended to both: (i) provide guidance on the functional perimeter; (ii) add additional products that are not captured by the general financial functions. The token, token system, function framework can also assist in assessing crypto ecosystem products against these specific financial product definitions.

47. The process of assessing crypto products against the functional perimeter (or a specific definition of financial product) is no different than the process for any other product. The regulatory status of a token system can be determined in the normal course of legal advice in respect of any facility and its function. However, the results of such an assessment will often depend on whether the token system:

    (a) involves intermediaries or agents performing functions pursuant to promises or other arrangements (**intermediated token system**) – see **Part C**; or

    (b) involves functions being performed by crypto networks in the absence of promises, intermediaries, and agents (**public token system**) – see **Part D**.

54 The definition of 'facility' is broad. It includes any intangible property and a term of any arrangement (whether or not the term is formal, written, implied or required by law, or legally enforceable). Two or more arrangements may be taken to constitute a single arrangement (see **Annexure 1**).

A high-level taxonomy

48. The functions associated with crypto assets can be categorised in multiple different ways.[55] Common methods include categorisation by high-level 'types',[56] associated behaviours,[57] technical features,[58] and intrinsic value.[59] The existing taxonomies are helpful in reaching an overall understanding of the universe of crypto tokens. They demonstrate clearly that crypto assets are not a homogenous asset class. They also demonstrate that there are clear financial and non-financial crypto assets and uses for crypto networks.

49. However, no existing taxonomies map to the Australia's financial services framework. While it may be possible to create an exhaustive, bespoke crypto asset taxonomy, this paper proposes a high-level taxonomy of four product types that can be grouped under the two kinds of token systems:

    (a) for intermediated token systems:

        (i) crypto asset services

        (ii) intermediated crypto assets

    (b) for public token systems:

        (i) network tokens (a type of crypto asset)

        (ii) public smart contracts (including some crypto assets created using smart contract tokens).

50. The reasons against creating an exhaustive taxonomy for crypto asset services and intermediated crypto assets include that their possible functions are effectively as broad as the possible functions of any contractual or social arrangement.[60]

51. The reason against creating an exhaustive taxonomy for network tokens and public smart contracts include that their possible functions are effectively as broad as any 'computing function'.[61]

52. The breadth of possible functions means the application of a more fulsome taxonomy in the context of regulation may have some drawbacks, including inconsistent regulatory treatment, co-mingled regulatory supervision responsibilities, and the opportunity for domestic regulatory arbitrage.

---

55 P Freni, E Ferro and R Moncada, 'Tokenomics and blockchain tokens: A design-oriented morphological framework', *Blockchain: Research and Applications,* 2022, 3(1), 100069; and L Oliveira et al., 'To Token or not to Token: Tools for Understanding Blockchain Tokens', *International Conference of Information Systems (ICIS2018)*, San Francisco, USA, 12 December 2018.

56 E.g. cryptocurrencies, decentralised finance tokens, meme tokens, stablecoins, governance tokens, etc.

57 E.g. speculation, yield generation, payments, investment, attestation, etc.

58 E.g. database structure, consensus type, fungibility, Turing-completeness, block size, etc.

59 E.g. no value (unbacked), redeemable for money, entitlement to dividend, means of exchange for network resources, etc.

60 The reference to social relationship refers to the definition of 'token system', which includes 'social protocols' – such as the agreement between players in a Monopoly game that the various tokens have the meanings within the game as defined by the rules of the game (see **Part A**). Computer games built on crypto networks code these 'social protocols' into smart contracts – in a similar way to an online Monopoly program.

61 This is because 'general-purpose networks' are a type of computer described as 'Turing Complete', which means they can perform any computable function.

Consultation questions

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?

Answer: We have no 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) IIn 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?

C. Intermediated token systems

53. Intermediated token systems typically involve a promise or arrangement for functions to be performed by intermediaries or agents. The terms of the arrangement would typically (but not always) be set out in a legally enforceable agreement (i.e. a 'promise'). These types of products use or rely on crypto networks, crypto tokens, or smart contracts as *part* of the product.

54. Intermediated token systems have a unique role in the crypto ecosystem. They can facilitate 'functions' that crypto networks and smart contracts cannot. They are the link between crypto networks and the 'real -world'.[62] As described above, the possible functions of intermediated token systems are effectively as broad as the possible functions of any contractual or social arrangement.

55. One of the unique roles that can only be performed by an intermediated token system is creating links with the existing financial system. This includes facilitating trades between crypto tokens and fiat money (known as 'on-ramping' and 'off-ramping' from the crypto ecosystem). It also includes the issuance and use of crypto asset-linked debit and credit cards, and creation of crypto tokens that represent conventional financial instruments.

56. An intermediated token system can be a 'intermediated crypto asset' or a 'crypto asset service'. Both types can be assessed against the functional perimeter using the token, token system, function approach to determine whether they are financial products. They can also be assessed against specific financial product definitions.

Crypto asset services

This section describes how some existing crypto asset services may be financial products when mapped against the financial services frameworks. A separate consultation paper on Licensing and Custody arrangements will consider how crypto asset services should be licensed.

57. A crypto asset service is a token system that accepts crypto tokens as part of performing a function under a legal agreement or other arrangement. The relevant 'token system' (i.e. business protocols that facilitate the function) are typically not crypto ecosystem specific. They could be used to offer the same services for any non-crypto asset with a secondary market price (e.g. accepting a gold necklace as collateral for a loan or creating a marketplace for consumer goods). Examples of crypto asset services include lending and borrowing, fiat on/off ramping, crypto token trading, funds management, mining/staking-as-a-service, gambling, and custody.

58. Crypto asset services are considered first in this paper as they are by far the most common way for consumers to get exposure to crypto assets. They also typically involve 'custodial'[63] relationships between consumers and service providers. As noted by OECD, the major failures during the recent crypto market downturn related to entities with clear centralised control over

62 The term 'real-world' is used in this paper to mean anything external to a crypto network.

63 The term 'custodial' is typically used to refer to any service where a token holder does not retain control of their crypto assets. This contrasts with holding a crypto asset directly (i.e. self-custody) or when using some smart contracts that provide analogous services in a non-custodial manner.

user assets (e.g. BlockFi, Celsius, FTX, and Terra/Luna).[64] Accordingly, there is a strong need for consumer protection to be addressed in the context of crypto asset services.

59. Customers of crypto asset services will not necessarily interact with or use crypto assets or crypto networks directly. The arrangement will typically involve a customer transferring crypto assets or fiat money to a service provider who will then credit the consumer's account (i.e. a 'custodial wallet'). The consumer's account would then be maintained by the service provider using an internal database. In these circumstances, consumers rely on the service provider maintaining crypto asset reserves that match the values attributed to customer accounts.

Crypto asset services as financial products

60. A crypto asset service can be considered against the functional perimeter or any of the specific definitions of a financial product (e.g. a mining/staking-as-a-service arrangement could be structured such that it is 'managed investment scheme', or a lending and borrowing service could be structured such that the arrangements are debentures or other securities).

61. Whether a crypto asset service is a financial product will depend on the terms and functions of the arrangements that constitute the service. However, despite many crypto asset services having clear economic or financial functions, it can be unclear which class of financial product they may fall within. Service providers may use complex or obscure arrangements that further complicate the assessment. This has led to situations where very similar products are offered by compliant and non-compliant service providers simultaneously.

62. Accordingly, the consultation questions below seek feedback on whether any arrangements should be specifically included in the definition of 'financial product' to either: (i) provide guidance on the functional perimeter; or (ii) add products that fall outside the general financial functions.

Crypto asset services as financial services

63. This paper does not consider financial services specifically. However, financial services are closely tied to the concept of 'financial product'. Broadly, the concept of 'financial service' in the *Corporations Act* is defined by reference to separate activities. Those activities relevantly include: (i) providing financial product advice; (ii) dealing in a financial product; (iii) making a market for a financial product; and (iv) providing a custodial or depository service.[65]

64. If a 'crypto asset service' is provided in respect of crypto assets that are financial products, the service provider would likely be providing a 'financial service' and subject to the relevant Australian financial services licence and other provisions of the *Corporations Act*. Existing examples of crypto asset services that are licenced financial service providers include:

    (a) businesses licenced to offer crypto token derivatives (e.g. options, futures, and contracts for difference); and

    (b) operators of ETFs that provide retail investors exposure to crypto tokens (e.g. a Bitcoin ETF).

64 OECD, 'Lessons from the crypto winter: DeFi versus CeFi', *OECD Business and Finance Policy Papers, 2022.*

65 See *Corporations Act*, Part 7.1 Div 4.

Intermediated crypto assets

65. An intermediated crypto asset is a crypto asset where the link between the crypto token and the token system is created by legal agreement or other arrangement. Linking a crypto token to an asset is sometimes described as 'tokenising' or making an agreement or asset 'programmable'. The link could simply be a term of an agreement or other arrangement that states that the function will be performed for any token holder.

66. The relevant 'asset' in respect of an intermediated crypto asset is often a bundle of rights or expected functions linked to a specific crypto token under a contract, deed, or other arrangement. In these cases, the crypto tokens are used as a record keeping device.[66] The 'assets', if they have the relevant connection to Australia, may be captured by a range of existing regulatory frameworks.

67. Examples of assets connected to crypto tokens include rights or licences in relation to event access or subscriptions, intellectual property, reward programs, consumer goods and services, fiat money, non-financial assets, government bond coupons, and units in a member-directed venture capital fund.[67]

Wrapped 'real-world assets'

68. Most 'intermediated crypto assets' (by value) involve an arrangement for a specific crypto token to be redeemable for fiat money that is held by the crypto token's creator.[68] These arrangements create crypto assets that are a type of 'stablecoin' (sometimes described as 'fiat-backed' stablecoins).

69. However, an arrangement can 'back' a token with any existing item, goods, product, or asset in the same way (e.g. by making a promise that a specific crypto token is redeemable for an item, good, product or asset that is held by the issuer). Crypto assets 'backed' in this way can be broadly referred to as 'wrapped' real-world assets.

70. **Example 1** is a stylised description of a fictional 'wrapped AUD', which is intended to represent a generic fiat-backed stablecoin on a public crypto network.

> **Example 1:** wAUD is a (fictional) crypto token. Its issuer advertises that it is backed 1:1 with Australian dollar deposits in an Australian bank account. The terms and conditions for the wAUD token state that the issuer promises to: (i) sell 1 wAUD for $1; and (ii) buy 1 wAUD for $1. The issuer creates (i.e. 'mints') the wAUD at the time of sale. The issuer destroys (i.e. burns) wAUD when it buys it back.
>
> wAUD is a smart contract token. It was created by the issuer using an open-source smart contract library. All functions necessary for a person to use or accept wAUD as payment or

66 In the same way as a registry entry or physical token is often used.

67 For examples of 'event tickets and subscription' see Australian Open (ARTB), 'intellectual property' see CryptoPunks (PUNKS), rewards programs see Starbucks Odyssey, 'consumer goods' see Penfolds wines x Blockbar (BTL), 'money' see Circle (USDC), 'non-financial assets' see Perth Mint (PMGT), 'coupon payments' see Ondo Finance (OUSG), 'units in a fund' see The LAO LLC.

68 As at 18 January 2022, the total value of all fiat-backed USD stablecoins is approximately US$137.2 billion. See The Block Dashboard.

collateral (i.e. transferability, authentication, and counterfeit resistance) are a default feature of the smart contract that was used to create the token.

Holders of wAUD use it (e.g. transfer it) by interacting with the smart contract on a self-serve basis. As a standard smart contract token, wAUD is interoperable with other smart contracts (e.g. its users can trade it using an 'automated market maker' or set up 'salary streaming').[69]

The stability of the wAUD to its 'peg' (i.e. its secondary market price) is effectively delegated to profit seeking arbitragers.[70] These actors ensure price stability by (i) buying wAUD at a discount on the secondary market when the price is below $1 (to sell to the issuer for $1) and; (ii) buying 1 wAUD from the issuer for $1 when the secondary market price is above $1 (to sell on the secondary market for a profit).

71. The relevant 'arrangement' in the example above involves a bundle of contractual rights created by the terms and conditions agreed to between the issuer and its customers.[71] It appears to fit within the broad definition of a facility. It can be assessed against the functional perimeter in the same manner as any non-crypto product. It could also be assessed against any specific definitions of financial product.

72. The relevant 'token system' in the example above includes all the 'real-world' internal business protocols implemented by the issuer to facilitate the issuance and redemption of wAUD. As with most intermediated crypto assets, an identical product could be created using physical tokens. A very similar product could also be created using a conventional database maintained by the issuer. However, a conventional database would require the issuer being responsible for clearing and settlement, managing accounts for all users, ensuring the security of database, etc. In the case of wAUD, the issuer has delegated all these business protocols to a simple, standard-form smart contract.

73. Accordingly, wAUD is an example of a product issuer using crypto networks and smart contracts to automate or remove the need for certain business protocols. While the technology used by an issuer to create a product is an internal business decision (and may not be a relevant factor in considering a product against the functional perimeter), the technology choices may be a relevant factor under other legal and regulatory frameworks. Accordingly, the overall product would also need to be assessed against these frameworks in the same way as any other product.

Other 'real-world assets'

74. Other 'real-world assets' include promises made in respect of crypto tokens that do not relate to any underlying asset held by the issuer. Examples include: the arrangements between a computer game developer and players that 'in-game' crypto token 'items' will have certain properties within the game, and the arrangements between an event ticket issuer and purchaser that a crypto token ticket will facilitate access to an event. The relevant 'asset' is the promise or other arrangement.

69 For an example of 'salary streaming' see Llamapay.

70 W Farrington, 'Stablecoin arbitrage: Everything you need to know', currency.com website, 13 May 2022.

71 But not necessarily between the issuer and all token holders (see sub-section on 'rights not accruing to holder', below).

75. **Example 2** below describes a real type of intermediated crypto assets that appears to have a financial investment function. They involve crypto tokens in a record keeping role only. The issuers are conventional corporate entities. An identical arrangement could have been created with physical tokens. A similar arrangement could have been created using a registry.

> **Example 2:** In 2017–18, several crypto asset exchange providers held public sales of tokens.[72] A common selling point with these tokens was a suggestion (but not necessarily a binding agreement) that the issuing exchanges would use the money raised to develop their business – with a portion of future revenue from the business being used to repurchase the same tokens on the open market at regular intervals.
>
> These repurchased tokens are typically taken out of circulation by the exchange permanently (this process is known as 'buy-back-and-burn'). Some of these exchanges have directed tens or hundreds of millions of dollars in business revenue to these repurchases in the years following these token sales.
>
> The actions of some of the crypto exchanges that conducted these token sales suggest that they did not consider themselves to be strictly bound to a buy-back-and-burn agreement (as there are examples of significant adjustments made in their buyback plans). However, the absence of an enforceable contract does not mean an absence of a facility.

76. These arrangements can be assessed against the functional perimeter in the same way as any non-crypto product. For example, the definition of a 'facility' may be wide enough to cover these loose 'buy-back-and-burn' arrangements. If so, the facility can be assessed against the general financial functions. The definition of 'makes a financial investment' (one of the general financial functions) appears to be a close fit. These facilities can also be assessed against any specific definitions of financial product.

Regulatory and policy issues

Rights not accruing to holder

77. In Example 1, the link between the fictional wAUD token and the underlying asset (the right to sell wAUD to the issuer for $1) is created by a simple legal contract in the form of the wAUD terms and conditions. A person acquiring the wAUD token on the secondary market or receiving it as payment may not be a party to this contract (and may therefore not have a right to sell the wAUD to the issuer for $1). In these cases, the non-party token holders can only convert to dollars in the secondary market – where they are exposed to supply-demand driven price fluctuations. An absence of arbitragers, or significant frictions or failures in the arbitrage process (e.g. inability of the issuer to quickly meet redemption requests), may cause instability in the secondary market price of the token.

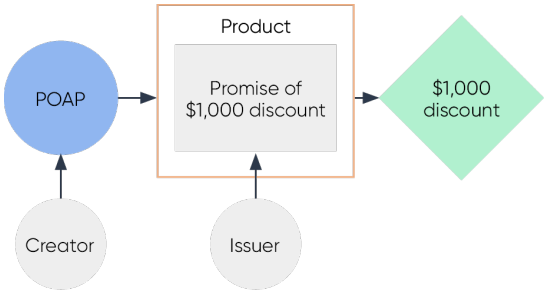
72 For example, see FTX, 'FTX Token Whitepaper (FTT)', Whitepaper.io website, 2020.

78. While proponents of 'tokenisation' point to benefits of increased liquidity and efficiency of transfers and settlement, the complexity described in this section impacts various legal and regulatory frameworks, including in the areas of contract law, consumer law, financial services law, AML/CTF laws, and sanctions laws. If this growth of 'real-world assets' continues in line with some expectations,[73] there may be a need for increased clarity and ultimately reforms to ensure financial stability and positive consumer outcomes.

Identifying products and issuers

79. The separation of the concepts of 'crypto tokens' and 'token systems' is important in the context of crypto assets. **Example 3** describes a fictional scenario that highlights the distinction between a crypto token creator and a crypto asset issuer.

> **Example 3:** Thom attends the 'FinTech Conference' every year. In 2022, the organisers arranged for 'Proof of Attendance Protocol'[74] (POAP) crypto tokens to be available for conference attendees. Thom claimed his POAP using the QR code provided at the conference.
>
> In 2023, a competing conference (the 'RegTech Conference') has been scheduled at the same time as the FinTech Conference. The organisers of the RegTech conference offer a $1,000 discount to anyone with a 2022 FinTech POAP to encourage attendees to their competing event.
>
> Thom sells his POAP to Haydn for $500 on an NFT marketplace.



80. The crypto token was created by Thom in 2022 (using a public smart contract published by the organisers of the FinTech Conference). The POAP was a 'keepsake'. The fact he created it proves he attended the event.[75] Thom was able to sell the crypto token in 2023 because a separate, arrangement (i.e. 'asset' or 'discount product') was connected to his existing crypto token. The 'issuer' of the discount product was the RegTech conference organisers.

81. The 'token, token system, function' can be used to ensure any regulatory obligations and responsibilities fall on the correct 'issuing' party.

---

73 J Eyers, 'Australia Readies to Ride $32trn "Tokenisation" Wave', *Australian Financial Review*, 1 July 2021.

74 A POAP is an NFT keepsake. They are typically linked to an image with an event logo.

75 These types of tokens have an 'attestation' function.

Identifying the terms of the arrangement

82. The terms of the arrangement linking a crypto token to its underlying asset may not always be publicly available. For example, the wBTC token is a crypto token that represents BTC on non-Bitcoin networks for the purposes of interoperability. It is a type of wrapped real-world asset (with the relevant 'asset' being the right to redeem 1 wBTC for 1 BTC). However, despite there being around US$3.7 billion wBTC tokens in circulation (and it being available for purchase on multiple crypto asset trading platforms), the precise terms of the arrangement linking the wBTC token to the asset are not clear.

83. This can cause difficulties with assessing a token system against the functional perimeter or any specific definition of financial product. Moreover, the strength of the arrangement (i.e. the type of legal instrument used to create the link between the crypto token and a bundle of rights) might be relevant to token holders in a number of ways, including: (i) how (and if) individual holders can exercise rights; (ii) the likelihood that the crypto token will maintain its peg (if it relates to a 'wrapped' real-world asset); and (iii) various issues that would arise in the event of the insolvency of the issuer.

84. The following questions aim to understand the challenges that exist and test how the existing regulatory framework might apply to intermediated crypto assets and crypto asset services.

Consultation questions

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?

Would this mean regulating asset backed stablecoins indpendently based on the the asset it is peggged too? i.e., treating comodity backed assets as comodities instead of stablecoins?

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?

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?

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?

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?

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?

D. Public token systems

85. Public token systems do not involve a promise that an intermediary or agent will perform a function in the future. They involve functions being ensured by a crypto network directly. This is enabled by two key practical innovations.

    (a) First, that public crypto networks can be used as neutral, independent infrastructure for creating transactional relationships between parties who do not know or trust one another.[76]

    (b) Second, that smart contracts *on public crypto networks* can be used to create and implement 'economic mechanisms'[77] that operate without the need for an intermediary.[78]

86. Public token systems are unique in that the transactional relationships are created by parties themselves – typically by using the same free open-source software simultaneously. The software enables the parties to create crypto tokens that represent their transactional relationship. These crypto tokens will typically provide their holders with a factual ability to perform functions in future (e.g. an ability to unlock a smart contract full of stablecoins if certain pre-conditions are met). This factual ability may exist in parallel to any legal rights or obligation, but it is ultimately ambivalent to them (i.e. the factual ability will exist regardless of a conflicting legal right).

87. The following two types of products are considered as part of the public token system analysis:

    (a) crypto tokens that are created as part of the 'consensus mechanism' on public crypto networks, but that are used by holders for various other functions (**network tokens**)[79]

    (b) smart contracts (and their associated crypto tokens) that are created for the purpose of enabling unknown parties to enter transactional relationships (**public smart contracts**).[80]

88. A consideration of the legal and regulatory issues relating to network tokens and public smart contracts is set out below.

Network tokens

89. Crypto networks are complex, experimental systems. They use a combination of technology and principles from the fields of computer science, cryptography, and economics.[81] One of the 'economic' components is the 'network token'. Network tokens are essential components of any *public* crypto network.[82] They are created by the network itself to reward specific network participants who contribute to ensuring all participants agree to the same database.

---

76 While innovative in its application, it is not a new idea (see D Chaum, Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups, University of California, Berkley, 1982).

77 An economic mechanism is a mathematical structure that models institutions (e.g. an auction, an exchange, a marketplace, a set of standards, organisations, etc (see L Hurwicz and S Reiter, *Designing Economic Mechanisms*, Cambridge University Press, Cambridge, 2006).

78 While innovative in its application, it is not a new idea (see N Szabo, 'Formalizing and Securing Relationships on Public Networks', *First Monday*, 1997, 2(9)).

79 These types of tokens are sometimes called 'exchange tokens' or 'native tokens'. Examples include BTC for the Bitcoin network, ETH for the Ethereum network, and ADA for the Cardano network.

80 A well-known public smart contract protocol is Uniswap v2. It is described further below.

81 The academic discipline that focuses on studying these systems is known as 'cryptoeconomics'. (see J Brekke and W Alsindi, 'Cryptoeconomics', *Internet Policy* Review, 2021, 10(2)).

82 Z Liu et al., 'A Survey on Blockchain: A Game Theoretical Perspective', *IEEE Access*, 2019, vol. 7, pp. 47615-47643.

90. The function of a network token from the perspective of a token holder will typically differ depending on whether the associated crypto network is:

(a) designed for the primary purpose of maintaining a secure ledger of network tokens (a '**cryptocurrency network**') or

(b) designed for the primary purpose of being a secure platform for developing software (a '**general-purpose network**').

Cryptocurrency network tokens

91. Cryptocurrency networks are (or were originally intended to be) peer-to-peer payment infrastructure – with the network tokens being a new type of 'currency'. Examples of cryptocurrency network tokens include BTC (for the Bitcoin network) and LTC (for the Litecoin network). These networks are *not* designed to host the types of smart contracts considered in this paper.

92. From the perspective of a token holder, the primary function of a network token on a cryptocurrency network is transferability. If the token has a secondary market price, the transferability function could be used to exchange it for something of value.

93. Many people buy cryptocurrency network tokens in the expectation that their secondary market price will appreciate (i.e. as a speculative investment). However, they are also used by some holders to store wealth (i.e. as a 'store of value') or to make payments (i.e. as a 'medium of exchange'), particularly in emerging economies.[83]

94. Whether or not cryptocurrency network tokens involve financial products will depend on the individual cryptocurrency network. They are not all sufficiently alike to consider them together. The following paragraphs describe the process of considering them against the functional perimeter.

95. If a public crypto network is *not* a facility, it is not a financial product under the functional perimeter. If a public crypto network is a 'facility', the speculative and payment functions could, for example, be assessed against the 'making a financial investment' or 'making non-cash payments' general financial functions. However:

(a) the 'makes a financial investment' function does not necessarily apply simply because an asset generates a return for a holder (e.g. gold and real estate are not financial products because they do not involve a return generated by the use of the purchase money by another person)[84]

(b) the 'makes a non-cash payment' function does not apply to exchanges of value between willing parties that do not afford the holder any *right* to make a payment.[85]

96. If these exclusions described above apply in the context of a specific network token, the crypto network is not a financial product under those general financial functions.

83 I Aderinokun et al., 'Letter in Support of Responsible Crypto Policy', Letter from Human Rights Foundation, 7 June 2022.

84 Corporations Act, s 763B.

85 See *Corporations Act*, s 763D.

General-purpose network tokens

97. General-purpose networks are crypto networks capable of hosting smart contracts. If they are public crypto networks, they will have network tokens for the same technical purpose (i.e. consensus) as cryptocurrency networks. As these network tokens are also transferrable, they can also be the subject of speculation, held as a 'store of value' or used as a 'medium of exchange'. Accordingly, the same analysis in respect of cryptocurrency networks can apply to general-purpose networks. Examples of general-purpose networks include the Ethereum network, and the Solana network.

98. However, network tokens on general-purpose networks are often intrinsically connected to one further function – the factual ability to publish or interact with smart contracts. This function is typically ensured by the relevant network's 'fee market mechanism'.

Fee market mechanisms

A user interacts with crypto networks (e.g. transfers crypto tokens) by sending a digitally signed message to the network containing processing instructions (see **Annexure 2** for details). Crypto networks do not have an unlimited capacity to process user instructions and store user data. Their capacity to do so is a limited resource.

A **fee market** is the 'economic mechanism'[86] used by a public crypto network to price and allocate its own resources.[87] A **network fee** is the price users pay to consume network resources.[88] The price paid by users will typically depend on how much of the network's resources are consumed by user's instructions and the current demand for those resources.

While fee markets exist on cryptocurrency networks, they have a critical role on general-purpose networks because they ensure it is economically unviable for a user to create a smart contract that uses the entire capacity of the network. Network fees therefore act as a 'tragedy of the commons' solution and as a protection against 'distributed denial of service' (DDoS) attacks.

As network fees are paid by users for all interactions with public crypto network and smart contracts, all users of general-purpose networks are required to have network tokens (e.g. a wallet containing smart contract tokens like stablecoins will need to also contain network tokens for those stablecoins to be able to be spent or used as payment).

Network fees are not paid by users when interacting with crypto tokens outside of a crypto network (e.g. when buying or selling crypto tokens through crypto asset services).

99. These fee markets are a kind of public token system. Whether or not they are 'financial products' will depend on the individual general-purpose network. They are not all sufficiently

86 An 'economic mechanism' is a mathematical structure that models institutions (e.g. an auction, an exchange, a marketplace, a set of standards, organisations, etc)

87 T Roughgarden, 'Transaction Fee Mechanism Design', in proceedings of the 22nd ACM Conference on Economics and Computation (EC '21), Association for Computing Machinery, New York, NY, USA, July 2021.

88 The dollar denominated cost of a network fees will further depend on the secondary market price of the network token. This can be used as a measure of the economic demand for a crypto network's resources (see https://tokenterminal.com).

alike to consider them together (e.g. they can be algorithmic or auction-based, and discretionary or non-discretionary).

100. If a 'fee market' is not a facility, it is not a financial product under the functional perimeter. If a fee market is a facility, it can be assessed against the general financial functions in the same way as any other product. For example, it could be considered against the definition of 'non-cash payment facility'.

Public smart contracts

101. Smart contracts exist on a spectrum from 'intermediated' to 'public'. At one end of the spectrum are the smart contracts used by intermediaries in providing a service (i.e. as part of the intermediated token systems described in Part C). This is currently the most significant end of the spectrum (by value of associated crypto assets) because it includes smart contracts used by large corporate entities – most notably, stablecoin issuers.[89]

102. At the other end of the spectrum are *public* smart contracts, which are used by parties to remove the need for an *intermediary*. This is the smallest category (by value of associated crypto assets) of the four products in this paper's high-level taxonomy. It includes various smart contract protocols and smart contract tokens *on public crypto networks*.

103. However, not all smart contracts on public crypto networks are *public* smart contracts. A smart contract on a public crypto network can be fully intermediated and permissioned (e.g. usable only by authorised customers of a business),[90] or fully intermediated but partly permissionless (e.g. a stablecoin that is freely transferable but that can be frozen but its issuer).[91]

104. A *public* smart contract can be created to perform any computable function. The most common functions appear to fall into three broad categories: (i) interoperability; (ii) economic; and (iii) coordination. An example of each is provided below. Further detail is set out in **Annexure 3**.

Interoperability mechanism: The smart contract associated with 'wrapped Ether' (wETH) can be described as an interoperability mechanism. It is a simple, immutable public token system published for a technical purpose.[92] It performs two functions: (i) accepting ETH in exchange for wETH; and (ii) accepting wETH in exchange for ETH. The smart contract is a publicly available, self-serve system that does not involve a counterparty.[93] It is incorporated into many smart contract protocols, which are used by multiple smart contract applications.

Economic mechanism: The smart contracts associated with the Uniswap protocol are a type of *economic mechanism*. When used by several participants, the protocol establishes a method for traders (demand-side users) to swap crypto tokens against pools of liquidity contributed by 'liquidity providers' (supply-side users).[94] Demand-side users pay 'swap fees', which are routed to supply-side users to incentivise them providing liquidity into the pools.

89 USDT (US $70 billion), BUSD (US $16 billion) and USDC (US $41 billion).

90 Compound Labs, Inc, 'Compound Treasury', website, n.d.

91 Circle Internet Financial Limited, USDC Terms | Legal & Privacy, Circle, 12 October 2022.

92 The purpose of wrapping ETH is to make it interoperable with smart contracts. ETH is a network token was intended to be used to pay for network fees and cannot natively interact with smart contracts.

93 Stephen, Formally Verifying The World's Most Popular Smart Contract, *Zellic Blog*, 18 November 2022.

94 H Adams et al, 'Uniswap v3 Core', *Uniswap website, n.d.*

The protocol is a publicly available, immutable self-serve system that is incorporated into several smart contract applications.

Coordination mechanism: A 'Moloch DAO' is type of smart contract protocol used by individuals who do not know each other to make collective investments into crypto assets. It enables users to contribute crypto tokens (e.g. stablecoins) into a pool in return for crypto token 'shares' (representing their contribution to the pool). Those 'shares' give the holders a factual ability to control the pooled funds, which is exercised *exclusively* through a smart contract mechanism that recognises these shares are 'keys'. Users can coordinate to unlock the funds for some joint purpose, or individual users can redeem their share of the pool at any time.

105. Between the two ends of the spectrum are smart contract protocols that provide various levels of control to an external entity. It includes multiple scams, Ponzi-like schemes,[95] or systems that involve economically functionless, inflationary 'staking'.[96]

106. However, along the spectrum are also a small number of attempts to implement a form of 'trust engineering'[97] or 'trust solutions'[98] (i.e. the use of smart contracts to replace conventional 'real world' system components with unbreakable rules encoded in smart contracts).

107. These protocols will typically incorporate 'coordination mechanisms' into the design of the product, which in some cases mean an individual or group of individuals (e.g. a 'decentralised autonomous organisations' (DAOs)) has some control over the protocol. The level of 'control' is often intentionally limited (i.e. to non-core components of the system with limited impact on existing users). However, it can be difficult to determine whether or not these protocols are truly intermediary-less without auditing the underlying code. The coordination mechanisms created for these purposes are described in Annexure 3.

108. Smart contract protocols that implement economic mechanisms are often referred to as part of the 'decentralised finance' (DeFi) or 'open finance' ecosystem. There have been several experimental crossovers between regulated entities and protocols in the decentralised financial space. For example, Société Générale-Forge used crypto tokens backed by home loans (OFH) to open a 'collateralised debt position' with DeFi protocol MakerDAO and create synthetic stablecoins (DAI).[99]

95 J Alexander, 'Of Smoke and Mirrors, Part 1 ', Medium (18 January 2022).

96 J Fish, 'ApeCoin & the Death of Staking', *Cobie* (Substack newsletter, 21 April 2022).

97 Patrick McCorry, 'Why Are Cryptocurrencies Interesting?' (Mirror, 23 March 2022).

98 H Peirce, 'Remarks before the Digital Assets at Duke Conference', website for the *US Securities and Exchange Commission* (9 November 2021).

99 See SG-Forge, 'Security Tokens Refinancing] MIP6 Application for OFH Tokens', MakerDAO Forum, October 2021.

Decentralised finance

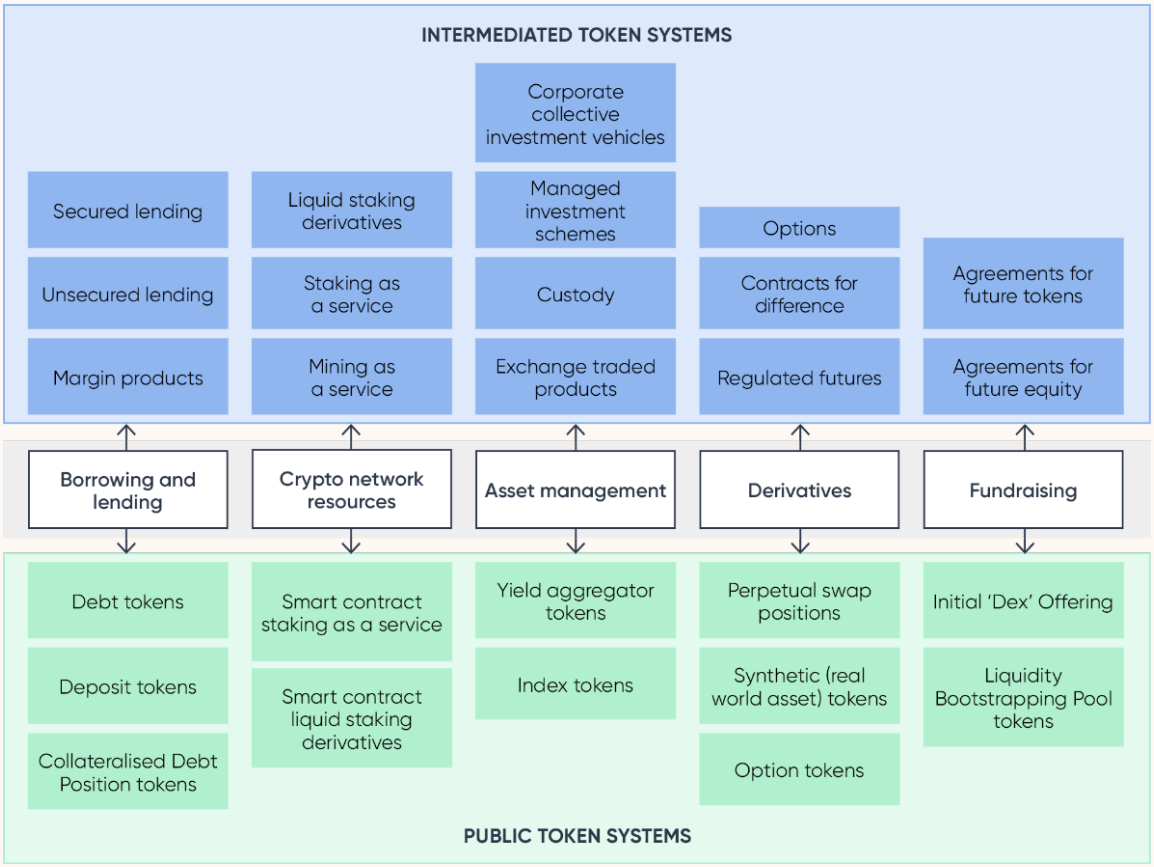
This part of the ecosystem is a niche and risky market with interesting properties in terms of efficiency, transparency, accessibility, and composability.[100] The smart contract protocols used in DeFi each fall somewhere on the spectrum described above.

In some cases, the relevant 'decentralised finance' products might closely match the description of a specific financial product in the *Corporations Act*, but there can be difficulties with some of the language used in definitions.

For example, the *Corporations Act* defines a 'derivative' as an arrangement under which a *party* provides consideration at a future time to *someone*. A derivative is 'issued' when a *person* enters the *legal relationship* that constitutes the derivative. In the context of a self-serve smart contract mechanism that replicates the economic functions of a derivative, the references in legislation to arrangements, people, parties, and legal relationships may pose challenges for the regulatory perimeter.

Figure 3 is a comparison of smart contract-based products or protocols that might be able to be described as public token systems (in green) and analogous products available from traditional financial intermediaries or through intermediated token systems (in blue).

Figure 3: Examples of Intermediated and Public Token Systems



100 F Schär, "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets," Federal Reserve Bank of St. Louis Review, Second Quarter 2021, pp. 153-74.

Regulatory and policy issues

109. These two categories of crypto products (network tokens and public smart contracts) cause several issues for legal and regulatory frameworks. The issues are deeper than whether these products are 'financial products' because the existing regulatory frameworks create regulatory boundaries, obligations, protections, and regulatory powers to be applied in the context of products that involve promises, intermediaries, and agents. Many of these do not map to public token systems.

110. In addition, the relevant risks of interacting with public token systems may not map to the protections provided under the current regulatory frameworks. For example, the risk that an economic function will not be ensured by a smart contract-based *mechanism* may be different to the risk that the same function will not be facilitated when supported by a contractual-based *promise*.[101]

111. While smart contracts are often touted for the removal of counterparty risk, this may be replaced by or aggravate a user's exposure to:

    (a) technology risks (e.g. a 'bug' in smart contract code)[102]

    (b) model risks (e.g. an unsound economic mechanism)[103]

    (c) compliance risks (e.g. blacklisting by smart contract applications)[104]

    (d) unknown risks (due to the experimental nature of these systems).

112. However, without conduct rules and effective enforcement mechanisms, markets can tend toward harmful practices (including conflicts of interest, anti-competitive conduct, and unequal access to information).[105] While some of these issues may have technical solutions using crypto networks and smart contracts, many may not. This could ultimately lead to a decline in investor trust and participation in the market.

113. While traditional policy and regulatory levers are available for a large portion of the crypto ecosystem (i.e. intermediated token systems), in the pockets of the ecosystem where functions are truly being ensured by public, self-service software, a fundamentally different approach may be required.

114. The following questions aim to commence the process of understanding what a financial regulatory framework might look like in a future where these unique elements of the crypto ecosystem continue to grow and develop.

---

101 F Schär, 'DeFi's Promise and Pitfalls', *International Monetary Fund: Finance and Development*, September 2022.

102 R Browne, '"Accidental" Bug May Have Frozen $280 Million Worth of Digital Coin Ether in a Cryptocurrency Wallet', *CNBC* (online, 8 November 2017).

103 C Beam, 'The Math Prodigy Whose Hack Upended DeFi Won't Give Back His Millions', *Bloomberg Businessweek* (online, 19 May 2022).

104 C Gu, 'Growing List Of DeFi Apps Ban Tornado Cash Users', The Defiant (online, 16 August 2022).

105 C Crenshaw, 'Statement on DeFi Risks, Regulations, and Opportunities,, *US Securities and Exchange Commission* (9 November 2021).

Consultation questions

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?

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 regualtory frameworks?

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?

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?

Conclusion

115. This paper describes key concepts needed to build a shared understanding of the crypto ecosystem. The aim is to assist industry, regulators, and consumers in navigating the crypto ecosystem and its interaction with financial services laws.

116. The paper describes the concept of the *functional perimeter* – the broad, functional definition of 'financial product' in *the Corporations Act*, which is intended to be technology neutral, flexible, and innovation friendly. It also proposes a token mapping framework to assist in conceptualising how crypto products might fit within existing regulatory frameworks.

117. The token mapping framework defines the concepts of 'tokens', 'token systems' and 'functions'. A *crypto token* performs the record keeping role. It is analogous to a physical token or an entry in a registry. A *token system* is the business or social protocol, or mechanism. It is the steps taken to perform a *function* in relation to crypto tokens. A *function* is the product or benefit provided by a token system.

Insights

118. The crypto ecosystem is not a homogenous industry sector and crypto assets are not a homogenous asset class. The process of assessing crypto related products against the functional perimeter is no different than the process for assessing any other product.

119. A large portion of the crypto ecosystem is 'intermediated token systems', which involve intermediaries issuing crypto assets and providing crypto asset services. Some of these token systems are clearly facilitating general financial functions. Others are clearly not. However, some regulatory reforms (in addition to licensing and custody reforms) may be needed to ensure consumer protection and financial stability into the future.

120. A separate portion of the crypto ecosystem exists to enable users who are unknown to each other to form transactional relationships in the absence of intermediaries or agents. These relationships may involve the creation of financial or non-financial crypto assets that are fundamentally different to their intermediated counterparts. Accordingly, they may not fit within a range of existing regulatory frameworks. Without reforms and new regulatory approaches, some crypto products in this category may be fundamentally incompatible with the existing financial services regulatory framework.

Next steps

121. Feedback is sought on the consultation questions throughout the paper to inform policy development. A complete list of consultation questions can be found at Annexure 4. This paper is open for feedback until 3 March 2023.

122. The Government will propose a framework for custody and licensing for public comment in mid-2023. Your feedback to the token mapping paper will be used to shape the development of these regimes.

Annexure 1. Legal and regulatory framework

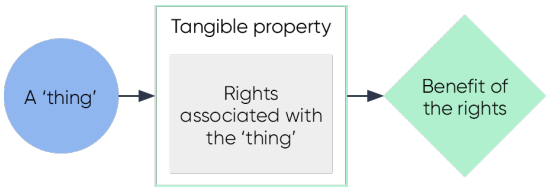
Property rights

123. In describing 'property', the High Court of Australia wrote:

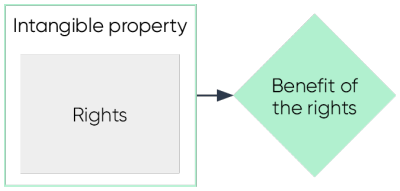
> *"…'[P]roperty' does not refer to a thing; it is a description of a legal relationship with a thing. It refers to a degree of power that is recognised in law as power permissibly exercised over the thing. The concept of 'property' may be elusive. Usually it is treated as a 'bundle of rights'".*[106]

124. The concept of 'property' is divisible into 'real' property and 'personal' property. Real property is the bundle of rights associated with land and its fixtures (i.e. real-estate). Personal property is divisible into 'tangible' and 'intangible' property.

125. 'Tangible' property is a bundle of rights associated with a physical 'thing'. The 'thing' exists independent of the law. The 'property' is created and governed by the law.



126. 'Intangible' property is a bundle of rights that must be asserted by taking legal action or proceedings (e.g. intellectual property, shares, some contractual obligations, and others).[107] The 'property' is created and governed by the law. There is no physical 'thing'.



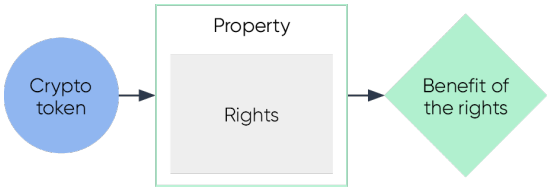
127. A crypto token itself is just data. It is unlike 'tangible' property – because it is not a 'thing' (it exists as information on many independent but identical databases). It is unlike 'intangible' property – because its inherent characteristics are not created or controllable by law.[108]

106 *Yanner v Eaton* (1999) 201 CLR 351. Another formulation is the 'Ainsworth' test (see *National Provincial Bank Ltd v. Ainsworth* [1965] AC 1175 at 1247-8, approved in, for example, *R v. Toohey; Ex parte Meneling Station Pty Ltd* (1982) 158 CLR 327 at 342.

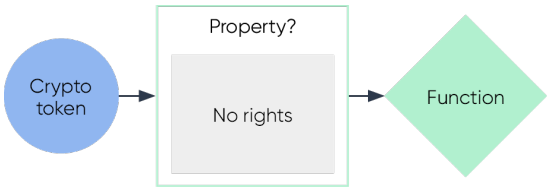
107 Australian Law Reform Commission (ALRC), Traditional Rights and Freedoms— Encroachments by Commonwealth Laws: Final Report, 2016, Chapter 7.

108 Law Commission (UK), Digital Assets: Consultation paper, 2022 [10.69].

128. However, when a crypto token is linked to a bundle of rights (e.g. a stablecoin may be linked to a right to redeem it for $1), the assessment is the same as intangible property (with the crypto token being used as a record keeping device – like an entry in a registry).



129. When a crypto token is not linked to a bundle of rights but rather to a token system that gives a holder the *factual ability* to do something (e.g. unlock a smart contract full of stablecoins) the crypto asset can be conceptually more difficult to describe as property.



Contractual rights

130. A contract is a legally binding promise or agreement.[109] A contract can be used to create property and 'non-proprietary interests'. Broadly, there are two types of contracts:

(a) a simple contract – an agreement between at least two parties. It requires each party to make a promise to provide something valuable as part of the agreement. Most contracts do not have to be in writing to be legally binding. They can be verbal or implied from the conduct of parties.[110]

(b) a deed – a declaration or promise made by one or more parties. A deed must always be made in writing. It can be made unilaterally.

131. Many crypto tokens are backed by some type of contract (e.g. USDC and wBTC are backed by agreements for them to be exchangeable for US$ 1 and 1 BTC, respectively).

Financial services regulation

Financial services regulatory framework

132. The financial services regulatory framework in Australia can be found across the *Corporations Act*, the *Australian Securities and Investments Commission Act 2001* (ASIC Act), and the *National Consumer Credit Protection Act 2009* (NCCP Act).

109 J Carter, *Carter on Contract*, Butterworths, Sydney 2002, paragraph [01.001].

110 Sometimes, some of these elements can be altered by statute.

133. The concepts of 'financial product' and 'financial service' have different definitions in the *Corporations Act* and *ASIC Act*. These concepts establish the regulatory perimeter for: (i) unconscionable conduct and consumer protections under the *ASIC Act*; and (ii) large parts of financial services and markets regulation under the *Corporations Act*. If a product or service does not meet those definitions, then it is not regulated by a range of important provisions in those Acts.

134. The inclusion of products and services relating to credit in the *ASIC Act* definitions of financial products and service creates overlap with the separate regulatory regime for consumer credit contained in the *NCCP Act*.[111]

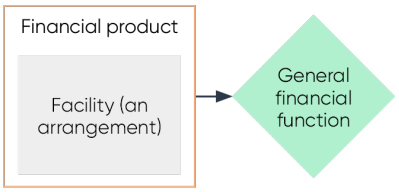
135. The concept of 'financial product' in the *Corporations Act* has many definitions. The general definition (i.e. functional perimeter) and several inclusions are outline below by way of example.

General definition of 'financial product' (functional perimeter)

136. Chapter 7 of the *Corporations Act* provides the general definition of a financial product. Under section 763A of the *Corporations Act*, a financial product is:

> *"(1) a facility through which, or through the acquisition of which, a person does one or more of the following:*
>
> *(a) makes a financial investment (see section 763B)*
>
> *(b) manages financial risk (see section 763C)*
>
> *(c) makes non-cash payments (see section 763D)."*

137. There are two distinct parts to this definition. First, there must be a **facility**. Secondly, that facility must be one that a person acquires for one or more of the three functions listed (**general financial functions**).



Facility

138. The definition of 'facility' is broad. It includes intangible property, a term of a contract, agreement, understanding, scheme, or other arrangement (whether or not wholly: formal, written, implied or required by law, or legally enforceable). Two or more arrangements may be taken to constitute a single arrangement.

General financial functions

139. If a facility exists, the second part of the assessment is to consider whether the facility is one through which a person does one of the three general financial functions. The three general financial functions are outlined below.

111 Australian Law Reform Commission (ALRC), Financial Services Legislation: Interim Report A, 2021, pg 276.

(a) *Makes a financial investment*: this function applies where a person gives money or 'money's worth' to another person for the purposes of generating a financial return or other benefit for the investor – in circumstances where the first person has no day-to-day control over generating the financial investment.[112]

(b) *Manages a financial risk:* this function applies where a person manages the financial consequences to them of particular circumstances happening; or avoids or limits the financial consequences of fluctuations in receipts or costs (including the value of receipts or costs).[113]

(c) *Makes non-cash payments*: this function applies where a person makes a payment otherwise than by the physical delivery of Australian or foreign currency in the form of notes and/or coins.[114]

Specific inclusions to 'financial product' definition

140. In addition to the general definition of 'financial product', there are lists of specific inclusions and exclusions of arrangements which are financial products.[115] The inclusions are intended to both: (i) provide guidance on the functional definition; (ii) add products that do not fall within the general definition.[116]

141. Two relevant inclusions that may apply to crypto assets and crypto asset services are managed investment schemes and derivatives. The definitions of each are outlined below, by way of example.

Managed investment schemes

142. A managed investment scheme is defined in section 9 of the *Corporations Act* and generally has three elements:

(a) people contribute money or money's worth to obtain rights (interests)[117] in the benefits produced by the scheme

(b) any of the contributions are to be pooled or used in a common enterprise to produce 'financial benefits'[118] or interests in property, for the people who hold an interest in the scheme (the members)

(c) the members do not have 'day-to-day control' over the operation of the scheme (but may have a right to be consulted or to give direction).

---

112 The purchase of something that generates a financial return does not necessarily constitute the making of a financial investment (e.g. gold and real property); and the mere act of giving money to another person may not necessarily constitute a financial investment (see *Corporations Act,* s 763B).

113 This function includes taking out insurance or hedging a liability by acquiring a futures contract or entering into a currency swap. It does not include employing a security firm as it is not a way of managing the financial consequences if thefts do occur. See *Corporations Act*, s763C.

114 This function applies where a person makes a payment other than by the physical delivery of Australian or foreign currency in the form of notes and/or coins. It does not apply where there is only one person to whom payment can be made by means of the facility. See *Corporations Act*, s 763D.

115 *Corporations Act,* s 764A and 765A. There are also inclusions and exclusions in regulations and ASIC class orders.

116 Revised Explanatory Memorandum, Financial Services Reform Bill 2001 (Cth) [6.69].

117 The definition of 'interests' in the *Corporations Act,* s 9 is broad. It includes a 'right' (whether the right is actual, prospective, or contingent and whether it is enforceable or not).

118 A financial benefit is not limited to profit or gain (see, *Brookfield Multiplex Ltd v International Litigation Funding Partners Pte Ltd* (2009) 180 FCR 11 [50]).

143. A 'scheme' may not be a managed investment scheme if a 'responsible entity' cannot be clearly identified or if the scheme is incapable of complying with the obligations in Chapter 5C of the *Corporations Act*.[119]

Derivatives

144. Chapter 7 of the *Corporations Act* defines derivative broadly as an arrangement that includes the following elements:

(a) a party to the arrangement must, or may be required to, provide at some future time consideration of a particular kind or kinds to someone

(b) that future time is not less than the number of days prescribed by law, after the day on which the arrangement is entered into

(c) the amount of the consideration, or the value of the arrangement, is decided by reference to (wholly or in part) the value or amount of something else such as an asset, an interest rate, an index.

145. A derivative is 'issued' when a "*person enters into the legal relationship th*at *constitutes the financial product"*.[120] Each person who is a party to a financial product that is a derivative and that is not acquired on a financial market is taken to be an issuer of the derivative.[121]

Australian crypto asset regulation

146. While this paper primarily focuses on the financial services framework, there are several frameworks with different regulatory objectives that apply to crypto assets in Australia. The following table provides a non-exhaustive overview of the key frameworks.

Table 1: Overview of Australian crypto asset regulation

Regulator: ASIC **Relevant Legislation**: *Corporations Act, ASIC Act* If the crypto asset is a **financial product**, it will be subject to certain obligations and requirements under the *Corporations Act* and *ASIC Act*. This includes prohibitions on misleading and deceptive conduct or unconscionable conduct, "hawking" or pressure selling, requirements as to disclosure about the features and characteristics of financial products before sale, design and distribution obligations, and requirements for those financial products traded on financial markets.
Regulator: ACCC **Relevant Legislation**: Australian Consumer Law For crypto tokens that are **not financial products**, the provisions of the Australian Consumer Law could potentially apply, including prohibitions against misleading and deceptive conduct. Businesses may engage in conduct that involves a combination of financial and non-financial products or services. To address this potential overlap, in 2018, the ACCC delegated powers to ASIC to take action under the Australian Consumer Law relating to crypto tokens.

119 LCM Funding Pty Ltd v Stanwell Corporation Limited [2022] FCAFC 103.

120 See *Corporations Act*, s 761E(3).

121 See *Corporations Act*, s 761E.

Regulator: AUSTRAC

Relevant Legislation: *AML/CTF Act*

Digital currency exchanges are regulated by AUSTRAC under the *Anti Money Laundering and Counter Terrorism Financing (AML/CTF) Act* for the purposes of preventing and detecting money laundering and terrorism financing.

Digital currency exchanges must register with AUSTRAC and meet AML/CTF compliance and reporting obligations (including Know Your Customer requirements).

Regulator: ATO

Relevant Legislation: *Income Tax Act, Goods and Services Tax Act*

Investors in crypto tokens and other market participants are subject to tax laws. If an entity is carrying on a business in relation to digital currency, or as part of their existing business, or if they are accepting digital currency as a payment in business, the entity needs to consider any GST consequences that may arise.

Tax implications for investors flow from the underlying nature of the rights and obligations attached to the asset and the personal circumstances of the investor. Crypto tokens will generally be capital assets, meaning there could be capital gains tax consequences.[122]

122 For more details, see Australian Taxation Office (ATO), Crypto asset investments, ATO, 2022.

Annexure 2. Public crypto networks

This annexure provides an overview of a generic crypto network. It attempts to describe in simple terms the technical concepts that are relevant to other parts of this paper. It does not purport to describe all elements of crypto networks. It has an intentional bias towards public (blockchain) crypto networks (as these types of crypto networks are associated with the most industry and academic commentary).

Overview of public crypto networks

147. A public crypto network starts as a set of standard methods for receiving, sharing, processing, and recording data. These methods are known as 'protocols'. A crypto network is established when two or more individual computers run software designed to follow the same protocols. These computers are known as 'full nodes' or 'network participants'.

148. Some public crypto networks comprise thousands of full nodes running on consumer-grade computers in the homes of a portion of users. Other crypto networks have a few full nodes running on professional-grade computing servers. The protocols for each different network are unique. The protocols relevant for the purposes of this paper are identified and summarised below.

Digital signatures

149. A network user does not need to run a full node to use a crypto network. They just need an **address**. Data on a crypto network (including tokens) are associated with specific addresses.[123] An *address* is simply a large number that is mathematically derived from another *secret* large number (a '**private key**').[124]

150. A private key is chosen at random[125] from an immensely large set of possible numbers (e.g. a Bitcoin private key is a number between '1' and around '115 quattuorvigintillion').[126] It is astronomically improbable that a truly random private key could be generated more than once – whether by chance or repeated guesses. A private key is used to 'digitally sign' instructions before sending them to the network for processing. A private key can authorise the network to change data at any address it created.

151. A 'cold wallet' is a record of a private key that has not been exposed to an internet-connected computer (e.g. a piece of paper). A 'hot wallet' is a record of a private key that is (or has been) exposed to an internet-connected computer (e.g. a software application). A 'custodial wallet' is an internal account maintained by a service provider (i.e. it does not record private keys or sign messages).

152. Various forms of software exist that can assist in the process of choosing private keys, deriving addresses, displaying balances, and signing and sending messages to the network. These are typically referred to as 'software wallets.'

---

123 Re 'public-key cryptography' see P McCorry, '*The 'Crypto' in Cryptocurrency*', *Mirror*, 30 March 2022.

124 These 'large numbers' are usually displayed in 'hexadecimal' format rather than decimal to keep them shorter.

125 The randomness is extremely important (secure methods usually involve dice, a calculator and paper (see W Swanson, '*Creating Bitcoin Private Keys with Dice*', *Swanson Technologies*, 2014)).

126 The precise figure is 115,792,089,237,316,195,423,570,985,008,687,907,852,837,564,279,074,904,382,605,163,141,518, 161,494,337 (for context, the estimated number of atoms in the Milky Way galaxy is a much shorter number).

Data processing

153. The instructions that a network can process are determined by its protocol design. A cryptocurrency network may only accept simple instructions (e.g. 'spend token at address *x* to address *y*'). A general-purpose network may accept more complicated instructions (e.g. 'check data at address *x*, use algorithm stored at address *y* to calculate a value to store at address *z*').

154. All full nodes on the network receive, process, and record the results of every instruction sent by users and other full nodes. When nodes follow the same protocol, they will reach the same results independently – creating multiple versions of the same shared database (**shared database**).

155. A node operator cannot be forced to follow a particular protocol when updating their version of the shared database. They are free do as they choose (e.g. delete a rival's data/tokens or create millions for themselves). However, full nodes that do not agree on the state of the shared database will ignore each other. These situations are called '**forks**'.

156. Forks are part of the data security model of crypto networks. If a full node is faulty or malicious, it will fork into a new network and have no impact on the rest of the full nodes.[127] The integrity of a public crypto network's data record relies on the existence of at least one honest/non-faulty full node.

157. Accidental forks occur continually due to faults in individual nodes. Intentional forks are used for planned upgrades. A 'contentious fork' occurs when a large group of node operators refuse to follow an updated protocol that another large group of node operators start following. In these cases, the old and new networks exist simultaneously. After most forks, users have access to their same addresses (and data/tokens) on both networks. In rarer circumstances, an intentional fork might be used to 'roll back'[128] or allow 'invalid entries onto'[129] the shared database.

Consensus and incentives

158. Nodes following the same protocol will not reach the same result of processing unless they process user instructions in the same order as each other. In a public crypto network, there must be at least one node responsible for proposing an 'ordered list' of user instructions (**consensus node**).[130]

159. Consensus nodes are not 'trusted' to act as intermediaries. A consensus node (or group of consensus nodes) cannot force the full nodes to violate the protocol (e.g. arbitrarily create, delete, or spend tokens). It is a common misconception that 51 per cent or more of consensus nodes can collude to force invalid changes to a public crypto network's shared database. However, a consensus node can censor users by refusing to include their transactions in the ordered list (and a large enough group of consensus nodes can cause significant damage to the operation of the network).[131]

---

127 M Maler, Learn the Blockchain Basics – Part 1: Determinism, Hackernoon website, 25 June 2021.

128 K Segdwick, Bitcoin History Part 10: The 184 Billion BTC Bug, Bitcoin.com website, 28 February 2019.

129 S Falkon, The Story of the DAO – Its History and Consequences, Medium, 24 December 2017.

130 Hasu, J Prestwich and B Curtis, A Model for Bitcoin's Security and the Declining Block Subsidy, Medium, Oct 2019.

131 Trail of Bits, '*Are Blockchains Decentralized?: Unintended Centralities of Distributed Ledgers*', Report prepared for *Defense Advanced Research Projects Agency (DARPA),* June 2022.

160. In a public crypto network, the role of consensus node is shared to prevent reliance on a single actor.[132] Sharing the role of consensus node is a technical problem in computer science. Consensus methods used in conventional distributed systems can be circumvented.[133] The solutions used by crypto networks include energy intensive puzzle games ('proof-of-work') and capital-intensive token lockups ('proof-of-stake').[134]

161. Consensus nodes are incentivised to perform the role with distributions of newly created network tokens at regular intervals. A public crypto network's consensus protocol uses network tokens and game theoretical principles to ensure the reward for honest participation in the network is more profitable than the potential benefit of mounting certain dishonest attacks against the network.

Fee markets

162. A public crypto network relies on nodes contributing private resources (e.g. internet connection, processing power, and digital storage). These resources are finite – with some portion being consumed each time user instructions are processed. Crypto networks measure their available resources in units (called 'gas' or 'weight').

163. A public crypto network that does not 'price' its resources is giving a private benefit to users at a socialised cost to node operators (i.e. a 'tragedy of the commons' scenario). Unpriced (or under-priced) resources expose networks to conventional system attacks (e.g. 'distributed denial of service').[135] A network's 'fee market' is the economic mechanism used for pricing its own resources (**fee market**).[136]

164. A simple fee market mechanism is an auction that prioritises user instructions that offer the highest price per gas/weight unit. The price of gas/weight is denominated in the crypto network's native token.

165. Some crypto networks use more complicated fee market mechanisms.[137] These mechanisms may be designed to solve several technical or economic issues, including the dilutive nature of the network tokens created and issued to consensus nodes as incentives.[138]

166. The consensus nodes are ultimately responsible for creating the ordered list of instructions. This role can be exploited for profit.[139]

---

132 Regarding 'decentralisation' see R Sai, J Buckley, B Fitzgerald and A Le Gear, '*Taxonomy of centralization in public blockchain systems*', *Information Processing & Management*, 2021, 58(4).

133 The circumvention occurs through a 'Sybil attack', see 'Sybil Attack: What It Is & the Threats It Poses to Blockchains', *Bybit Learn* (7 June 2022).

134 Regarding 'consensus mechanisms' see Wang et al, '*A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks*'.

135 See for example C Harper, 'Nano's Network Flooded With Spam, Nodes Out of Sync' CoinDesk online, 11 March 2021; and Guido, 'Nano (XNO): Network at a Standstill for Days Due to DDoS Attacks', Block-builders.net, 24 May 2022.

136 V Buterin, Blockchain Resource Pricing, Eth Research website, August 2018.

137 Tim Beiko, 'Why 1559?', *HackMD* (2021).

138 T Roughgarden, Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559, 2020.

139 Regarding 'problems with transaction ordering' see Daian et al, '*Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges*', *arXiv,* 2019.

Annexure 3. Smart contracts

Overview of smart contracts

167. A smart contract is not a 'contract' in a legal or plain English sense. The term was coined in a pre-blockchain era to mean technology that could *alleviate the need* for certain business protocols (e.g. standard form contracts, internal business controls, compliance controls, and administrative routines).[140]

168. The classic example of a primitive smart contract is a vending machine. Like a vending machine, a smart contract does not necessarily remove or replace any legal relationship between buyer and seller. However, it alleviates the need for:

    (a) some business controls (e.g. to prevent theft of coins by shop staff; or theft of drinks by customers)

    (b) some compliance controls (e.g. to prevent manipulated records)

    (c) some administrative routines (e.g. hiring, rostering, payroll, managing, etc).

169. A vending machine is a *primitive* smart contract because: (i) its rules can be broken (i.e. by stealing the products using force); (ii) its physical mechanisms can degrade (i.e. with time); and (iii) it can be manipulated by third parties.

Smart contracts on crypto networks

170. If hosted on a secure crypto network, smart contracts cannot be manipulated (although, bugs and bad designs can be exploited).[141] Smart contracts are structurally different than programs used in conventional computing. They comprise (i) a static block of computer code (i.e. an algorithm); and (ii) a dedicated internal database. A smart contract does not 'run' continually. A user provides inputs, and the host crypto network runs the algorithm and records its outputs. The algorithm may rely on data elsewhere on the shared database, and on the functions of other smart contract (i.e. they are 'composable').[142] All instructions are executed together in one snapshot of time (i.e. atomically).[143]

171. Smart contracts can be combined with legally binding, natural language agreements to create symbiotic 'smart legal contracts'.[144] However, the primary uses for smart contracts to date has been the creation of *protocols* that enable relationships to be governed by software *rather than law* (sometimes described as *Lex Cryptographia* – a new body of law').[145]

172. In these cases, users may have opted out of entering contractual relationships with other users and developers. However, no user or developer can opt out of the law generally. The use of

---

140 N Szabo, 'Formalizing and Securing Relationships on Public Networks', *First Monday*, 1997, 2(9).

141 F Schär, 'DeFi's Promise and Pitfalls'.DeFi's Promise and Pitfalls', *International Monetary Fund: Finance and Development*, September 2022.

142 P Tolmach et al, 'Formal Analysis of Composable DeFi Protocols' [conference paper], *Financial Cryptography 2021 International Workshops.*

143 M Bech et al, 'On the Future of Securities Settlement', *Bank for International Settlements Quarterly Review,* 1 March 2020.

144 S Wilkinson and J Giuffre, 'Six Levels of Contract Automation: The Evolution to Smart Legal Contracts – Further Analysis', March 30, 2021.

145 A Wright and P De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', *Open Journal of Applied Sciences*, 2015, 11(10).

smart contracts likely still involves the creation of legal relationships (e.g. duties of care). It does not exclude overarching public law (e.g. criminal law, tax law, regulation, etc).

Smart contract protocols

Immutability and upgradability

173. Smart contract protocols can be immutable or upgradable (in whole or in part). Those parts that are upgradable may be controlled by an individual or a group of individuals (**protocol guardians**). A protocol guardian may control a smart contract through a 'coordination protocol' (such as a decentralised autonomous organisation (**DAO**) or multi-signature wallet).

174. Only two major smart contract protocols in the decentralised finance space appear to be fully immutable.[146] Immutable protocols (or protocols with very limited updatability) cannot be wholesale upgraded – improvements are made by publishing an entirely new version of the protocol. The old versions will always continue to exist alongside the new one for anyone who wishes to use it instead (e.g. Uniswap v1/v2/v3 all exist and are operational).

175. Most smart contract protocols implement a form of selective 'trust engineering'[147], which allows protocol guardians to use an iterative software development cycle (e.g. iterative improvements and bug fixes).[148] These protocols are typically be designed to mitigate upgradability risk (e.g. by restricting upgrades to components of the protocol that would not enable protocol guardians to steal user funds, and/or adding frictions (such as time locks) that allow users to exit the protocol before changes are made).

176. A user who cannot read smart contract code will not be able to self-assess the upgradability risk of a protocol. Protocol guardians of major smart contract protocols will often engage professional smart contract auditing firms to publish reports on vulnerabilities in the code (including upgradability risk).

Coordination protocols

Decentralised autonomous organisation

177. A DAO is a crypto network-based system that enables people to coordinate and self-govern according to smart contract rules published on a public crypto network.[149] DAO membership can number tens of thousands of individuals across multiple jurisdictions. DAOs often attempt to avoid legal agreements by implementing unbreakable rules encoded in smart contracts. These rules can be used to protect DAO controlled assets, reduce the need for ongoing monitoring, and allow for the detection of fraud or other insider abuses.[150] Some DAOs have begun to explore and implement the concept of 'legal wrappers', which provide some form of limited

146 H Adams et al, 'Uniswap v3 CoreUniswap v3 Core', *Uniswap website*, March 2021 and *Liquidity*, 'Official Liquidity Documentation', Liquidity website, November 2022. H Adams et al, 'Uniswap v3 CoreUniswap v3 Core', *Uniswap website*, March 2021 and *Liquidity*, 'Official Liquidity Documentation', Liquidity website, November 2022.

147 Trust engineering is the discipline of defining the components of a protocol that require human trust to function and replacing it with an executable program (see Patrick McCorry, 'Why Are Cryptocurrencies Interesting?' (Mirror, 23 March 2022).

148 M Salehi, J Clark and M Mannan, 'Not so Immutable: Upgradeability of Smart Contracts on Ethereum', *arXiv*, 2022.

149 S Hassan and P De Filippi, 'Decentralized Autonomous Organization', *Internet Policy* Review, 2021, 10(2).

150 A Wright, 'The Rise of Decentralized Autonomous Organizations, [2021] Stanford Journal of Blockchain Law & Policy.

liability and the ability to enter contractual arrangements – but allow the operational parameters of the DAO to continue to be dictated by smart contract frameworks.[151]

178. A DAO framework can be created to implement any custom rules that can be enforced by a crypto network. However, many DAOs are created by relying on standard libraries of smart contracts.[152] They will typically be created to enable distributed control of another smart contract (e.g. a shared 'treasury' or 'smart contract protocol'). Control is often exercised through polls where ballots are cast by token holders.

179. Some DAOs are structured such that polls are non-binding – with results being implemented by trusted members of the community. Other DAOs are structured such that a poll that meets a pre-defined level of support is the sole method of taking an action (e.g. spending from a DAO treasury might require a majority of token holders to send signed messages to the crypto network with their approval). More complex methods can involve bicameral structures (with an action needing to be approved by trusted members of the community and the community as a whole).[153]

180. An interest in a DAO through holding a voting token (commonly known as a 'governance token') may be difficult to classify under existing financial services laws. They are not 'equity' in any traditional sense and they do not necessarily entitle holders to legal 'ownership' of the DAO controlled funds. However, DAOs can generate revenue for their token holders and many DAOs control 'treasuries' of crypto token valued in the hundreds of millions or billions of dollars.

Participatory DAOs

181. A participatory DAO (or project DAO) are DAOs that act as protocol guardians to a smart contract protocol. The relevant smart contract protocol could be economic mechanism (i.e. a DeFi protocol), or a social/community protocols, infrastructure protocols, or charitable protocols. Members of the DAO will typically contribute services (such as technical development or community management) in return for 'governance tokens'.

182. A participatory DAO may look somewhat like a co-operative business or a partnership. As all their financials are recorded on the crypto network's share database, they can provide real-time financial reporting for their community of members to review.[154] Several aggregator websites exist that generate financial statements and activity reports for DAOs based on public crypto network data.[155]

Investment DAOs

183. A common method for collective investments is a 'Moloch DAO'. It involves a person contributing funds (e.g. stablecoins) in return for non-transferrable 'shares'. Each contributor is then given a vote on the collective investment to be made, but has the opportunity to extract their portion of the pool, if they disagree with the choice of investment. These mechanisms have been used to rapidly raise significant funds.

151 Brummer, C. Rodrigo, S., DAO Strategy and Legal Wrappers, Paradigm (8 June 2022)

152 moreReese, 'A Pocket Guide to DAO Frameworks.', Tally (11 October 2022).

153 Optimism DAO, 'What Is the Optimism Collective?', *Optimism Docs* (6 December 2022).

154 For example, see MakerDAO – Dashboard.

155 For example, see Deep Dao – Organisations

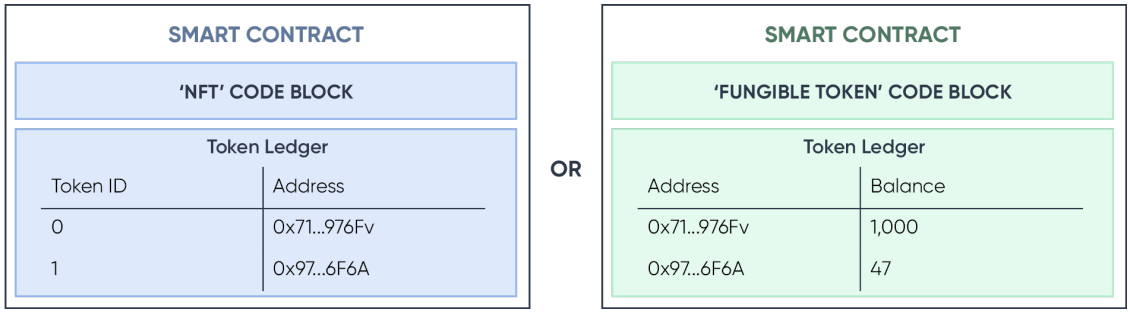
Interoperability protocols

Token standards

184. While there are multiple methods for creating crypto tokens,[156] the most common method is using a 'standard form' smart contract designed to create tokens (**smart contract tokens**). Any person comfortable using an internet browser is able to create a crypto token using a standard open-source library. There are over 3 million smart contract tokens across the three most popular networks.[157]

185. A standard form smart contract is 'published' with the code necessary to turn the smart contract's internal database into a token ledger. The separate token ledger maintains balances for the newly created token. The difference between a fungible token and a non-fungible token (**NFT**) is a slight change in how the smart contract database is structured (see **Figure 3**).

Figure 4: Fungible and non-fungible tokens



Economic protocols

186. Smart contracts that implement economic mechanisms are often referred to as 'decentralised finance protocols'. An economic mechanism is a mathematical structure that models institutions (e.g. an auction, an exchange, a marketplace, a set of standards, organisations, etc).[158] In theory, a smart contract can implement "*any computable economic mechanism without a trusted intermediary*".[159]

187. Protocols implementing economic mechanisms have been used to create intermediary-less ways for users to: (i) swap tokens (AMM protocols); (ii) lend and borrow crypto tokens (lending and borrowing protocols); and (iii) create synthetic assets (collateralised debt positions).

AMM protocols

188. One mechanism for swapping between two crypto tokens is a constant function market maker's 'bonding curve'[160] (also known as 'AMM').[161] An AMM relies on supply-side and demand-side users to operate. Supply-side users provide liquidity in a pool. Demand-side users pay fees for

156 Regarding 'token creation' see J Roth, F Schär and A Schöpfer, 'The Tokenization of Assets: Using Blockchains for Equity Crowdfunding' in Karen Wendt (eds), *Theories of Change*, Springer Nature, Switzerland, 2020.

157 Totals calculated from Ethereum (https://etherscan.io/tokens); Polygon (https://polygonscan.com/tokens); and BSC (https://bscscan.com/tokens).

158 L Hurwicz and S Reiter, *Designing Economic Mechanisms*, Cambridge University Press, Cambridge, 2006.

159 N Szabo, 'Formalizing and Securing Relationships on Public Networks'.

160 S Aramonte et al, Trading in the DeFi era: automated market-maker, *Bank for International Settlements Quarterly Review*, 6 December 2021.

161 Hasu, 'Understanding Automated Market-Makers, Part 1: Price Impact', *Paradigm Research,* 19 April 2021.

swaps. Fees are routed from the demand-side to the supply-side. AMM protocols have been used for over US$1 trillion of intermediary-less crypto token swaps.

Lending and borrowing protocols

189. Public lending and borrowing protocols are smart contract-based mechanisms for disintermediated borrowing. Smart-contract algorithms replace two key functions traditionally performed by a real-world intermediary in a loan agreement: interest rate setting and legal enforcement of the loan.

190. The protocol involves lenders (supply-side users) providing liquidity into a pool from which borrowers (demand-side users) can borrow. Demand-side users pay 'interest' to supply-side users (typically added to the debt rather than paid by the borrower directly). The interest rate is set through the natural market forces of supply and demand (e.g. an algorithm that applies low interest rates when there is low demand for the pooled assets and high interest rates when there is high demand for the pooled assets). [162]

191. The model adopted is similar to that of a pawn broker (e.g. no recourse loan). Borrowers lodge collateral greater than the value of the loan (i.e. overcollateralised). Should the value of the collateral fall below the 'loan to value' threshold stipulated in the smart contract, the collateral becomes publicly available for purchase at a small discount. The discount incentivises arbitragers (usually bots) to buy the collateral (to sell on the open market at market prices). The money from the sale of the collateral is routed back to the pool, and the borrower's debt is extinguished.

192. However, if the market moves too quickly and sale of collateral does not cover a borrower's debt, the pool may be 'underwater'. While lending and borrowing protocols fared better than the intermediated lending and borrowing counterparts during recent market volatility,[163] there are numerous examples of lending and borrowing protocols that are underwater.[164]

193. Aside from the decision to use the protocol, none of the steps described above involve discretionary actions. None of the large lending and borrowing protocols are fully immutable. They typically rely on a DAO as protocol guardian to approve certain changes to the underlying smart contracts (e.g. to add new types of collateral and lending markets).

Collateralised debt position protocols

194. Collateralised debt positions (CDPs) on the surface look similar to borrowing and lending markets. With both, the user lodges collateral and withdraws a different token, the difference being that CDPs create an entirely new token for withdrawal, rather than borrowing the assets of lenders.[165]

195. The new tokens created have no systematic use to those who do not have debt, but they can be assured that they will maintain value as those who own the debt will willingly buy the tokens when needed or when supplied at a discount.

196. The creation of many derivative similar products in DeFi take the form of tokens, the value of which is contingent on fluctuations in the value of one or more referenced assets or another

---

162 Aave, Borrow Interest Rate, last accessed 30 Jan 2023.

163 OECD, 'Lessons from the crypto winter: DeFi versus CeFi', *OECD Business and Finance Policy Papers, 2022.*

164 RiskDAO, Bad Debt Dashboard, last accessed 30 Jan 2023.

165 MakerDAO, Whitepaper: The Maker Protocol: Multi-Collateral Dai (MCD) System, MakerDAO website, 2020.

observable variable. Decentralised derivatives may reference a stock, commodity crypto asset, or cash flows on a business venture.

197. Tokenised derivatives may not make use of an intermediary like in traditional finance. Governance, maintenance, and auto-liquidation of collateral for decentralised derivatives are often controlled by smart contracts.

Revenue generating protocols

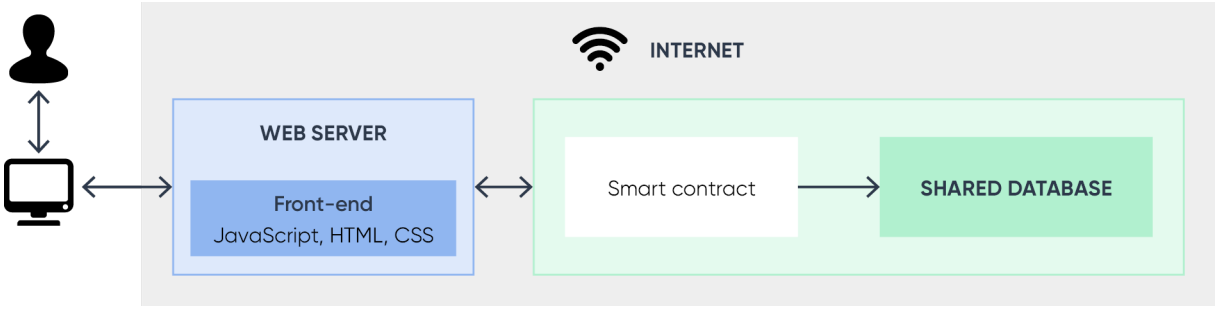
198. Smart contracts that collect fees from users can generate cashflows. In some cases, these fees are a necessary part of an incentive mechanism to make the protocol work (e.g. fees paid by users of AMMs that are directed to liquidity providers to incentivise liquidity). In other cases (where the smart contract protocol is created by a traditional business), the revenue may be directed back to an address controlled by the business (e.g. OpenSea marketplace for NFTs). In a few cases, the protocol revenue is distributed directly to the protocol guardian's governance token holders. Several aggregator websites exist that generate financial statements and activity reports for smart contract protocols based on public crypto network data.[166]

Smart contract applications

199. A smart contract application is a user facing interface (a website of program) that relies on smart contract protocols to provide functionality or services to users. A popular smart contract protocol will be accessible through a variety of smart contract applications (for example, the Uniswap AMM is used by wallet applications (e.g. zerion.io and zapper.fi), aggregators (e.g. app.1inch.com) and standalone platforms (e.g. instadapp.io and app.defisaver.com).

200. A smart contract application sits between a user and a smart contract protocol – allowing a user to interact with the smart contract through a standard webpage. Unlike a smart contract protocol, a smart contract application is often not immutable and will typically be controlled by an entity who controls the domain where the website is located.

Figure 5 – smart contract applications



166 For example, see Token Terminal and Messari Protocol Reporting

Annexure 4. List of consultation questions

All the consultation questions, posed in this paper, are listed below. Please provide your responses to the following consultation questions and include examples where relevant.

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

Answer:

The Government should be responsible for:

A) Setting the national policy of Australia with regards to crypto. This would include determinations on or ideas of:

- The type of crypto ecosystem Australia wants to foster;
- The types and volume of crypto business Australia wants to attract;
- The overall attitude to risk and how risk-taking or conservative Australia wants to be in different areas of crypto;
- The overall attitude towards innovation;
- The desired perception of Australia on the international crypto stage;
- The balance Australia wishes to strike between regulation and innovation;
- The level of resource (both financial and non-financial) that Australia wants to, and can, commit to making its vision for crypto regulation a reality;
- The type of crypto regulatory regime Australia wants to design, whether it be more prescriptive/rules based or outcome-focused with flexibility as to how outcomes are achieved/princples-based; and
- How a newly implemented, fully fledged crypto regulation regime would co-exist with the current AML/CFT requirements already in place for crypto businesses in Australia.

B) Following on from point A above, and taking the considerations into account, the Government should then work closely with regulators and policymakers to formulate and, on an ongoing basis, evolve regulation of the crypto ecosystem in Australia. This should include passing legislation and ensuring that any proposals can be implemented under/in conjunction with the country's existing relevant legislation (e.g., Corporations Act ASIC Act, AML/CFT Act, Income Tax Act, Goods and Services Tax Act, Australian Consumer Law, etc).

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

Answer:

Safeguards for consumers and investors should:

A) protect consumers and investors from the risks that exist in traditional finance

B) protect consumers and investors from the risks specific to crypto, whether they be as a result of the technology, a novel product/service, or the way an entity operates (centralised vs decentralised).

Safeguards for consumers and investors therefore need to take into account a number of factors: the technology used, the products/services offered and whether these are offered by a centralised entity, a decentralised protocol, or something in-between, whether existing safeguards from traditional financial services regulation provide appropriate protection, whether they can be tweaked, or whether a new type of safeguard is required.

Some elements of crypto asset activity by centralised businesses can and should be regulated in the same way as traditional financial businesses, e.g. ensuring proper risk management practices and

sound corporate governance are in place at the firm, ensuring fit and proper people run the business, having business continuity and disaster recovery plans in place, AML/CFT controls, firms having adequate financial resources, the gating of products/services based on risk and complexity, etc.

Some elements of crypto asset activity by centralised businesses, due to the technology used and/or products/services offered, need to be regulated differently or in new ways. For example, the processes and controls surrounding crypto asset custody and transfers, requirements for smart-contract code audits and what these entail, transaction monitoring methodologies (blockchain analytics), settlement arrangements, the content of risk disclosures and investor education, etc.

Some elements of crypto asset activity by decentralised businesses also need to be regulated in different ways. At the product level, DeFi and NFT businesses, for example, require a range of consumer and investor protections different to anything we have seen previously because of the way they operate. Similarly, decentralised protocols themselves will need to be regulated in a different manner (e.g. how these protocols meet KYC requirements, who is accountable to the regulator, etc) to traditional financial and traditional centralised crypto products and services. At a global level, these discussions are now taking place, but effective solutions are yet to be agreed upon or implemented.

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?

Answer:

In addition to the already mentioned solutions, such as appropriate disclosures and requirements for code auditing, consumer education and monitoring are important safeguards when it comes to scams.

Both firms and the regulator should have sections on their websites dedicated to issuing guidance on warning signs and what to look out for when encountering potential scams. This should be updated on a regular basis as new types of scams emerge in the crypto space.

The regulator should also have a team (wholly or in part) dedicated to conducting research and dealing with potential scams. This team should also be responsible for issuing public warnings relating to unregulated companies and potential scammers who are issuing false and misleading advertisements (e.g., stating they are regulated). A clear process should be in place so that the regulator has the powers to demand such scams cease activity, or to allow the regulator to collaborate with law enforcement to ensure that scams cease activity.

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

Answer:

The main protection in this area will be that regulated crypto token exchanges have a Token Listing Policy in place. This will detail the process by which a token is proposed for listing on the exchange, the due diligence and analysis that takes place on the token, the methodology by which the exchange determines whether a token is approved for listing or not, who at the firm is responsible for token listing decisions and review of the policy, timelines, implementation considerations, managing

conflicts of interest and inside information, as well as the process for de-listing token from the exchange.

Furthermore, crypto token exchanges should be required to adhere to clear and well thought out Marketing policies. The regulator should have oversight of the exchanges' Marketing policy and ensure that marketing communications are fair, clear and not misleading.

For exchanges listing their own native tokens, we would add:

For any offering of a native/ exchange's own token, the regulator could ask the exchange to submit a whitepaper, detailing the rationale for the token, relevant technical information, tokenomics, details surrounding allocations, pre or private sales and relevant vesting periods, use case(s), and investor rights and protections. The regulator would then be able to decide, based on its own criteria, whether to approve or deny the token.

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

Answer: No answer.

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

Answer:

Disadvantages - would the inclusion of "exclusive use or control" mean that crypto tokens (or networks) that are controlled by others fall outside of scope? For example, when a custodian (pure custodian, exchange, etc) holds a crypto token on behalf of a client - the client will have rights confirming ownership of that token, but the custodian will still have the exclusive control over it and will need to be the party that processes a transfer should the client request a withdrawal of their crypto token from the custodian ecosystem to their private wallet. What about when crypto tokens are held in multi-sig wallets (in a DAO or at an exchange, for example)? Who is defined as having "exclusive use or control" - it is no longer "*a person"*? What about when crypto tokens reside within smart contracts after a user of a service has sent them, do they still have "exclusive use or control"?

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?

Answer: No answer.

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

Answer:

A standalone regulatory framework that relies on a bespoke taxonomy has both pluses and minuses.

Two key elements of any effective regulatory framework for crypto are flexibility, so as to be able to keep up with an extremely fast-changing, young and developing space, and clarity, so that both firms and consumers know where they stand.

Unfortunately, the two often do not go hand in hand. Clarity is provided by specific definitions and clear perimeter setting, which then restricts flexibility when new types of crypto, crypto services or use cases emerge and evolve. Setting a wider or vaguer perimeter allows flexibility for the jurisdiction to react quickly and effectively to developments within the ecosystem but will lead to a lack of clarity for some firms and the services they offer, and for their consumers. It will also lead to some firms attempting to position themselves inside or outside of the regulatory perimeter, often on technicalities, based on what suits them best.

Creating a standalone regulatory framework that relies on an exhaustive bespoke taxonomy for crypto asset services and intermediated crypto assets could cause regulatory setbacks and stunt innovation. The crypto industry is evolving regularly, and new innovative ideas surrounding how crypto assets, smart contracts and their functions can be used are being continuously introduced. From a regulatory and policy perspective, it could be unnecessarily burdensome for the regulator to continuously review and define whether a particular service or product should fall under a different 'token system' and be subject to different frameworks/requirements, especially when new types of tokens and token systems emerge. This particular approach would no doubt have a significant impact on a regulators' resources and require expertise in complex niche areas for the purpose of identifying and implementing new requirements.

From a firm and consumer perspective, it would provide clarity initially, but then risk becoming outdated and losing clarity as the crypto ecosystem continues to evolve.

A standalone regulatory framework is not necessarily a bad idea, as it allows for the specific risks and evolution of the crypto ecosystem to be tailored to, whilst it will also help distinguish from other existing financial services frameworks and prevent regulatory overlaps. We feel that you can still have a standalone framework with a bespoke taxonomy, as long as the taxonomy is drafted in a way that provides flexibility or can be interpreted widely (with guidance that is easier to update if/when necessary).

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?

Answer: No answer.

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?

Answer:

Wrapped real-world assets should not get the same regulatory treatment as that of the asset backing it. Doing so would result in doubling and repeating regulatory efforts, whilst also then potentially encountering hurdles that the crypto element of a wrapped real-world asset would introduce. This is not to say that wrapped real-world assets should not get regulatory treatment, they should. Effective regulatory treatment would ensure that holders rights, especially regarding redemption of the wrapped asset for the real-world asset, are respected, that the stabilisation mechanism of the peg between the wrapped asset and the real-world asset is strong and maintains itself, and protections for investors if the issuer of the wrapped asset defaults.

Would this mean regulating asset backed stablecoins indpendently based on the the asset it is peggged too? i.e., treating comodity backed assets as comodities instead of stablecoins?

No, they would be treated as crypto as per the above.

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?

Answer:

Issuers should be subject to regular monitoring and reporting of the underlying good, product or asset, and there should be clear rules as to whether and what investments can be made using consumer assets (e.g. consumer gives 1 AUD in exchange for 1 wAUD, issuer then invests 1 AUD in commercial notes or liquid short term bonds, etc).

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?

Answer:

Yes, crypto asset service providers should advocate for transparency, and be required to have readily accessible information regarding consumer protection, which should include the arrangements underpinning crypto tokens on their platform.

Ensuring that clients are better able to understand the protocols and functionalities of the crypto tokens they are investing will better help them understand the risks and benefits of investing in crypto tokens and help them make informed investment decisions based on speculative assets. In order to achieve this, crypto asset service providers should ensure information on each crypto asset it offers is prominently displayed in a way that is clear, fair and not misleading; and presented in a way that can be understood. The information presented should include information regarding the DLT system/network used for each token and the nature and inherent risks involvedin the underlying technology generally and in the specific system/network used (e.g. dependency on third party or open source software and networks, or on protocols subject to indpendent consensus mechanisms). Information can be retrieved from protocol websites in the case of already existing and/or being well known, or directly requested from protocols if they are going through the listing process.

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

Answer:

Crypto asset service providers could ensure that token issuers have issued a crypto token white paper before being listed on the crypto asset service provider platform. Risk disclosures are also important.

More generally, restricting access to certain products and services based on their risk and complexity is a protective measure that achieves a good consumer outcome. For example, leverage/margin trading on crypto (either spot crypto or crypto derivatives such as futures and options) is risky and complex, and should therefore only be accessible to consumers who are able to understand and analyse the risks and mechanics of the leverage/margin trading. Firms could put appropriateness testing in place prior to permitting access to such a product, giving them comfort that consumers who do access it have displayed the appropriate level of knowledge, experience and understanding.

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?

Answer: No answer.

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

Answer: No answer.

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?

Answer:

Some appropriate measures could include the level of decentralisation of the public crypto network, the cost of attacking the network, the history of network security and up-time, the cost of transacting on the network, the adoption of the network, development activity and financial runway of the network (so as to determine the likelihood of it continuing to exist in the long term).

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?

Answer: No answer.

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?

Answer:
Firms should be required to comply with certain marketing and advertising standards and guidelines, such as content and language that should not be included in adverts and marketing communications, the types of client that can and cannot be targeted by certain businesses and/or products and services, and the type of information, disclaimers and disclosures that must be included in adverts and marketing communications. All of this will help protect consumers.
Part of this requirement should be that crypto businesses have clear and well thought out marketing policies in place, and that the regulator has oversight of these policies to ensure they are fit for purpose. These policies will mean that firms:

- have adequate oversight to ensure compliance with marketing and advertising standards and guidelines;
- have robust processes in place for the review and approval of marketing communications;
- ensure that any advertising produced is clear, fair and not misleading; and
- regularly review, and/or review based on certain triggers, the firms policies and processes in this area.

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?

Answer:

Amending legislation/regulation to bring smart contracts within the perimeter of existing regulatory frameworks. Only if smart contracts replicate services that are regulated. Or if there are identifiable central entities/people benefiting economically (gaining fees) from the deployment of the smart contract.

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

Answer: No answer.

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?

Answer:

The valuing of crypto tokens in over-collateralised lending, which can change quickly due to volatility, and in large quantities are subject to illiquidity concerns, as well as smart contract bugs, errors and hacks.

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?

Answer: No answer.

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?

Answer:

The main risks pertinent to using AMMs include smart contract code bugs, errors and hacks, the risk of impermanent loss for clients who choose to provide liquidity, and the withdrawal of liquidity from liquidity pools on AMMs. On the plus side, the way AMMs function lend themselves to better consumer protections in the form of more orderly liquidations and negative balance protection (if leverage is used), as long as appropriate controls are in place to prevent the quick/instant withdrawal of liquidity from liquidity pools. Depending on the level of decentralisation of the AMM service, it may be hard to regulate or hold people accountable for failures and losses (i.e. a code bug that causes a loss of client assets).

Crypto asset exchanges, on the other hand, present different risks in that they are centralised, and therefore are more subject to human error and/or theft, whilst they also present counterparty risk for consumers holding crypto tokens on the exchange (if they are mismanaged and fail as a business, consumers could lose their exchange holdings).

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

Answer: No answer.

Annexure 5. Glossary

Term	Meaning in this document
Automated Market Maker (AMM)	a smart contract-based, economic mechanism for intermediary-less swaps between crypto tokens
Blockchain	a type of crypto network where data is recorded in packages called blocks. Each block is 'chained' to the next in chronological order using a cryptographic hash.
Buy-back-and-burn	a 'feature' of a token sold to raise money for development of a business (often by a crypto asset exchange) – with a portion of future profit or revenue from the business being applied to repurchasing the same tokens on the open market at regular intervals. The repurchased tokens are typically taken out of circulation by the exchange permanently
Consensus node	a node with the responsibility for creating a list of user instructions for all nodes to process
Crypto	used commonly as an umbrella term for crypto networks, their various components, and the surrounding industry
Crypto asset	a token system that is intrinsically linked to a specific crypto token (the intrinsic link means the term 'crypto asset' is effectively an umbrella term for a crypto token and its associated token system). (See Part B: under 'essential concepts')
Crypto asset service	a token system that accepts crypto token in providing some function according to a legal agreement or other arrangement. The relevant 'token system' (i.e. business protocols that facilitate the function) are typically not unique to crypto assets.
Crypto asset trading platform	a trading platform where crypto assets can be bought and sold
Crypto network	a distributed computer system capable of hosting crypto tokens (See Part B: under 'essential concepts')
Crypto token	a digital token that can be 'exclusively used or controlled' by a person – despite that person not controlling the host hardware that stores the token
Cryptocurrency network	a crypto network that exists for the purpose of maintaining a secure ledger of network tokens
Cryptography	a science at the intersection of mathematics, probability, electrical engineering, computer science, and others that is concerned with the transformation of information for one or more of the following purposes: (i) data confidentiality; (ii) data integrity; (iii) authentication; and (iv) non-repudiation
Custodial service	any service where a token holder does not self-custody their assets. In the crypto ecosystem, the concept of 'custody' has a broader meaning than traditional in finance
Decentralised Finance (DeFi)	a financial (or financial-like) function performed by a public token system
Facility	the legal definition of 'facility' is broad. It includes intangible property, a term of a contract, agreement, understanding, scheme, or other arrangement (whether or not wholly: formal, written, implied or required by law, or legally enforceable)
Fee market	the economic mechanism used by crypto network for pricing its own resources
Fork	an event that occurs when one or more nodes that previously followed the same protocol as other begin to follow a different protocol. 'Accidental forks' occur continually due to faults in individual nodes. 'Intentional forks' are used for planned upgrades. 'Contentious forks' occur when one or more nodes refuse to follow an intentional fork
Functional perimeter	any 'facility' through which, or through the acquisition of which, a person does one or more of: (a) makes a financial investment; (b) manages financial risk; and (c) makes non-cash payments (together, the 'general financial functions').

Term	Meaning in this document
General financial function	under the *Corporations Act* a general financial function consists of one of the following: (a) makes a financial investment; (b) manages financial risk; and (c) makes non-cash payments
Governance tokens	tokens which can grant users the purported opportunity to become a partial owner and decision-maker in a DeFi protocol. Often issued as an incentive for network participation
Immutable	a state that once accepted, is impossible to unwind (however, the term 'immutable' in the context of crypto networks has a softer meaning. It refers to the requirement of strict global consensus (meaning that all participants must agree to the exact same data). A mature, highly distributed crypto network with thousands of participants will typically provide 'harder' immutability than a younger, less distributed network.167
Index tokens	a type of crypto token with a fundraising function that passively tracks a basket of crypto tokens
Intermediated token system	a token system that uses crypto tokens in their record keeping role but otherwise relies on something external to the crypto network to ensure the function (e.g. a contract, legislation, or other arrangement)
Network token	a type of crypto token that is essential to the architecture of a public crypto network (See Part D: under 'network tokens')
Node	any computer connected to a blockchain network is referred to as a node. A full node is a computer that can validate transactions and download the entire data of a specific blockchain. In contrast, a "lightweight" or "light" node does not download all pieces of a blockchain's data and uses a different validation process
Non-fungible tokens (NFTs)	representations of unique data. Each token is mathematically unique and unable to be fractionalised, unlike many fungible crypto assets. NFTs are commonly used to represent artwork ownership, however as they are just a data structure, potential use cases are wide ranging
On-ramp/Off-Ramp	an arrangement for trading between fiat money and crypto tokens
Private key	a large random number that can be used to 'digitally sign' instructions for changing data stored at any address that was derived from it
Protocol	a set of rules and procedures for receiving, sharing, processing, and recording data that a computer can follow to become a node (See Annexure 2: under 'overview of public crypto networks')
Protocol software	a type of software (often referred to as a 'protocol client') that is designed to follow a particular protocol to enable a person to participate in the network (See Annexure 2: under 'overview of public crypto networks')
Public token system	a token system that can perform a function without the involvement of promises, intermediaries, or the discretion of people
Shared database	a record of the transaction history of a crypto network maintained individually by computers following the same protocol
Smart contract	computer code that has been published to a crypto network's database, guaranteed to run in a predefined and deterministic manner without risk of intervention. See Part B: under 'key smart contract terms'
Smart contract application	a user facing application that combines one or more smart contracts, external data sources, and external servers to provide functionality or services to users
Smart contract protocol	a set of smart contracts used to define procedures for specific types of interactions between users without an intermediary
Smart contract token	a token created and maintained by a smart contract

167 In the earlier days of the two major crypto networks (Bitcoin and Ethereum) concerns of network participants around an 'immutable' action led to intentional 'forks' to revert that immutability (See **Annexure 2** under 'data processing protocols').

Term	Meaning in this document
Staking	the act of escrowing or 'locking' a crypto token with a smart contract (originally used to refer to 'staking' in a proof-of-stake crypto network but now broadly used to refer to any kind of escrow or 'lock' function)
Token	a physical or digital 'unit of information' that typically has a role in a token system designed to perform a function (See Part A: under 'essential concepts')
Token system	a token system is anything designed to ensure or facilitate a function (See Part A: under 'essential concepts')
Wallet	method of recording a set of private keys a 'cold wallet' is a record of a private key that has not been exposed to an internet-connected computer (e.g. piece of paper) a 'hot wallet' is a record of a private key that is (or has been) exposed to an internet-connected computer (e.g. a software application). a 'custodial wallet' is an account with a service provider (i.e. it does not record private keys or sign messages)