Fungible.Farm (AU)

Elastic.ventures (US)

[redacted]

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

By email only: crypto@treasury.gov.au

Reference URL: https://treasury.gov.au/sites/default/files/2022-03/c2022-259046.pdf

Thank you for the opportunity to provide feedback on the proposed regulation of crypto asset secondary service providers (**CASSPrs**).

My name is Brian Horakh. I am a recent emigrant from the US, California with my wife who is from Australia, and having only been here since the early days of covid during lockdown. Prior to arriving in Australia I did a critical systems Internet infrastructure & consulted for many of the US top-5 for 25 years, and most recently have been upskilling in technologies for the past 7 years on subjects including artificial intelligence and web3. I have also been more broadly very involved in open-source communities my entire life even from childhood (and I'm 46 now).

However, please excuse my US accent and overall approach to how I would suggest you approach this, presenting some out of the box ideas of "giant leap forward" type thinking since my nephew or niece will be playing with this someday. I am presently planning to do a crypto-coin ERC-1155 native decentralized autonomous organization registered either in the US or Australia based on the most-suitable jurisdiction.

This is divided into three sections. Part 1: I spend a bit of time on the first question & second question advocating for "word precision & finger protocol", then Part 2. direct short answers for 26 questions and then Part 3. expand on the ideas from the earlier - introducing what I see as a series of incorrect assumptions caused by the Australian language vernacular, an effect I call "Word Compression" and why that is potentially harmful if codified into regulatory law. In each case I try to ensure that I present possible solutions to how I would suggest you approach regulation given what little I know about the history of the country but knowing considerably more about how to use technology to address/solve issues in its shortcomings or undesirable behaviors & dodgy actors.

Thank you for your consideration and I apologize that I ran short of time to coalesce many of these thoughts.

I had no difficulty reading the consultation paper and had no difficulty understanding any part of the guidance. I found Appendix 1 "Appendix 1 – Overview of Australian crypto asset regulation" extremely

helpful.

1. Do you agree with the use of the term Crypto Asset Secondary Service Provider (CASSPr) instead of 'digital currency exchange'?

As an acronym, CASSPr is not hard to pronounce. Sounds like "Casper" and doesn't make my mouth hurt. That is the nicest thing I will say about it. I hope during this paper to deconstructively attack it like a strawman argument and hopefully advance your knowledge & awareness in this field to better inform your next steps.

I don't believe CASSPr is particularly useful in terms of identifying attributes across a very broad set of ideas. It is a very narrow term that is subsequently followed by assumptions, related to a singular aspect of the organizations that would normally fall under the ATO regulatory domain. However "the types of digital-currency-exchanges" are only the first type of crypto-entity that the ATO agency is presently interfacing with, this is the "tip of the spear" for crypto. There are many interesting open-source community projects in the DeFI (Decentralized Finance) which could accidentally be labeled or subject to a CASSPr - that concerns me. Specifically what concerns me is these more beneficial technologies will be squelched by ATO "Aussie word summarization", specific regulatory problems your agency faces today. CASSPr is perhaps better than DCE, but both terms lack specificity and are equally ambiguous. Digital Currency Exchanges or Digital Crypto Exchanges, Decentralized Coin Exchanges those which can exchange fiat to crypto-coins or crypto-tokens (not the same) are logically the first type of entity necessary to onboard users into the various protocols & which then subsequently allow enrollment & participation in web3, and later web4, etc..

I will first attempt to explain a "better" method to delineate & approach this, that would I believe would be a more useful & effective strategy related to what the role & goals and within the ATO's sphere and locus of control relating to "crypto-currency" regulation, web3 metaverse strategy - with the assumption that since you organizationally have a web2 website today - someday that may be upgraded to web3, and what steps can be made today to create a bridge .. i.e. while what I'm proposing may seem like a web3 strategy, I'm trying to point out very specific next steps to get ATO web 2.1 - which is the minimum compatibility level you should consider enacting any crypto-governance controls (even voluntary ones) after your organization & nation begins on the it's own web3 metamorphosis journey. How quickly the nation is able to do this will depend greatly on how onerous & restrictive the early legislative efforts are.

I will make points later for more specific classifications & distinctions for significantly increasing "word precision" (and later, why it is especially important for the ATO to counteract the effects of Australian "Word Compression"). I will advocate for adoption of industry 'well understood' known foundational technical specifications so that the AU federal government might obtain maximum benefit from the positives and mitigate the worst negative aspects of crypto (from what I believe is my view of how Australia - given my limited understanding of it's administrative & organizational structure might have missed better solutions.)

I would like to apologize in advance for how technical some of this is. Let's start with an assertion that AU sovereign Governance & oversight is optional in crypto. I do this for the pro crypto-anarchists who might read this and suddenly freak out! Yes, sovereign oversight will always be optional & best-effort in crypto (it's just how decentralized things work, no single individual controls the network - an organization driven by a non-custodial smart contract does what the programmers told it to, I can run a blockchain network with my friends over a VPN tunnel steganographic messages encoded in the cat fur of Internet memes and there little any government can do to prevent that) .. But I'm also going to challenge the assertion/generally held belief (at least in Australia) that 'crypto-anarchy' is the default-state. And first I'm

going to describe an approach toward AU friendly easy-as crypto governance as extraordinarily voluntary & helpful, and assistive “high utility” trust signals injected directly into the network for entities under your jurisdictional domain. I say this here, explicitly in summary for readers who want me to get right to the point and don’t want to read the whole thing.

I envision the role of ATO as a cyber-shepard helping both individuals & institutional investors equalize the effects of asymmetric information (usually the scammer knows it’s a scam, but the person being scammed doesn’t, that is an example of asymmetric information). The ATO should inform Australian’s (or even the entire globe) who they *might* be able to trust and who they definitely shouldn’t trust (according to the ATO), or who may be acting dodgy in an effort to “short circuit” problems & limit the size of the craters these rug-pulls might create in the national economy as adoption grows.

This is not only very technically feasible, I hope to demonstrate it is straightforward and easier than the approach you are taking. How participation can be offered & induced on a voluntary basis. The role of government is to do advanced planning in preparation to mitigate or respond to problems, in crypto this can be best illustrated by regulatory kill switches and fail-safes “guard rails”. This is a “install fire sprinklers” sort of crypto-contract code & zoning-compliance types of controls are going to be discussed, broadly how to go about implementing them in the least harmful & most useful way to support all present & future cryptographic blockchains applications.

If a company is being investigated, you can also change their status, provided the ATO has a programmatic way to publish this information as a ‘micro-service’. I don’t need to believe scammers because I should *technically* be able to query/validate their claims are or are not signed by the ATO and confirm what the entity's relationship with the ATO is in terms of known-observable (non-custodial) or custodial compliance officer attested regulatory compliance.

(my systems protocol level inquiry to the ATO system itself should suggest registration/unknown entity, log the request and be somewhat reactive to slow or prevent theft/rug-pulls by after the 10th or 100th occurrence in a day/week/month can be used to provide data-driven decision making).

This makes other less sophisticated nations, or those who have failed to adopt/embrace second generation crypto-currencies that have smart-contracts). Distinguishing first generation “bitcoin” from second generation “virtual machine” - smart contract capability, introduces an important aspect of governance ‘options’ that should be explored. The intention of this aspect is to put a series of de facto ‘slowing burning fuse’|in limiting scope of potential scams and ensuring minimal levels of ‘finger on the short-circuit or gasoline button’ controls to pause & inspect (or even time travel & reverse, OR approve+accelerate as a voluntary service). Present global crypto systems have no sovereign controls, but as soon as a control is available it’s risk of failure, when described specifically and accurately, etc. action can be actuarially assessed and underwritten in trinary risk markets (if secondary markets are crypto-assets, then trinary markets [by your definition of CASSPr] are probably dealing with risk & insurance, leverage & lending, etc.). In this sense my argument is for a more holistic approach assuming all entities in technical domains with write access to the contracts have access to asymmetric information.

By implementing entities in an organizational graph database each new governance capability is simply a word or technical term or phrase which can be represented in a matrix as either applicable or not.
For those terms which are applicable & controls available adopted are each binary Y/N or T/F. Each answer can also have two other categories: short ‘tweet sized’ reasons why such term does not apply OR Other governance functionality not implemented out-of-scope exception. Suddenly the ability to describe & classify entities by their technical attributes and governance protocols suddenly becomes ‘real’.

By preparing a decision tree ‘identification’ matrix for deciding which terms to apply to which technology

services, company organizational structure & underlying protocols. Without using this level of technical detail in your rules they will always be overly ambiguous and subject to incorrect interpretation.

Personally speaking, crypto will not go truely mainstream until there are some levels of safety control. Most people embrace control structures hat keep them safe (i.e. not-crypto anarchy, which most 'average' Australains 'rule abiding' persons don't actually want). The societal benefits of smart-contracts, etc. can't happen until ATO or some other sovereign foreign entity can demonstrate the value of providing voluntary tools to shut down 'scammers' exploiting wallets (i explain how this is technically possible, and challenge some 'well held, generally true but also false, provided such consent & participation is induced on a voluntary basis 'service catalog' the the ATO should be providing starting with giving crypto "the finger" address for one or more services. I explain how finger is both a protocol and a concept, i.e. "having your finger on the button" (as in a kill switch). By building a consensus of other agencies in other countries, the code & systems can be forked and shared using the GIT version control system as other countries see the benefits and adopt similar to (or perhaps identical to) Australian methods. Even in the case of similarity, the git version control system to codify your rules as executable libraries will allow ideas to be 'cut and paste' (using a mechanism called pull requests and merges) that are nearly identical to the ones organizations governed by smart contracts must use internally. (such that the law, and the technical terminology - i.e. the "command" or "function/method name") are consistent across all parties.

Voluntary safety measures using established already globally deployed Internet protocols are what the ATO should be planning - do not "let the industry regulate itself", provide a registry file or micro-service and denote the stage in the process an organization is in (literally they should be able to register and obtain provisional status immediately). Files in smart contracts always "compile" to the same sequence of letters and numbers called a cryptographic hash or signature - this is a fundamental truth of every blockchain & cryptographic signature. I won't explain all the nuances of asymmetric public keys - beyond saying this is very well understood, forward compatible technologies.

These governance & broadcast protocols I'm referring to are 'finger' [an Internet protocol] was originally designed in 1977 and provides the first known implementation of foundational naming/identity services existing more than a decade prior to the web. The web is designed for humans, but finger is designed for universal human/or programmatic access using a syntax sugar (such as suggesting a filename via finger, specifying the extension). Finger is actually easy-as to implement, a flexible "future proof" proven approach. Finger+DNS for zero-trust key exchange, programmatic query/lookup. Any crypto-currency running on the Internet should be able to easily implement the finger protocol (or frankly, they have NO business being a crypto-currency) - it is non-graphical, purely text based and public which is why finger is well suited for this application. It is a standard feature of every operating system since the early 1980's in compatibility so it predates the blockchains by 30 years and provides a very low barrier to entry for both the ATO and the adoptee's.

I hope to describe an approach to national naming conventions for technology regulation & within the Australian Tax Office for validation & registration purposes and avoiding unnecessary acronyms in both protocol documentation & rules. The resources creating acronyms and classifying what is and isn't an acronym isn't nearly as effective as actual executable code or implementable technical protocol standards (for services).

Broadly your agency could consider adopting methods for vernacular parity with the crypto-industry 'self-identifying' in terms of which validation process & protocols. Go back to the fundamental services - agree to respond to a finger or to perform two way fingers (bi-directional fingering) for more complex forms of key exchange. To explain - the finger response could be necessary to go/no-go key-to-unlock and perform certain actions within programmatic non-custodial smart-contract. Finger is a popular old-school way of sharing/validating security keys, and it is presented conceptually.

Another application of finger - is that both national and international finance companies who may or may not be stating they are following compliance, last reviewed, etc, other known information such as insurance & banking status, etc. in an API (Application Programming Interface) accessible format. A large company such as a JP morgan might only implement the AU ATO technical governance controls such as finger protocol on the ERC-20 wallet(s) that are designated/governed by it's AU entity within Australia (especially when both wallets are voluntarily registered as 'honorable' AU citizens or entities), this allows smarter decisions to be made by providing more information to the network and brings more value to Australian citizenship, possibly NZ (or in my case, hopefully also eligible for those with future-permanent resident status). My point is, have a provision for international companies who may have to follow one or more international standards and explicitly say which situations are impermissible/inappropriate for regulatory inclusion in your voluntary safety & investor compliance program.

That is an example of how the ATO can provide some bastion of safety & meet the industry half-way. While it is nice to ask companies to follow and certify their security, it is not the same as regulating companies where they may be many different versions, but when we talk about L1 blockchains there actually won't be many that see daily use - especially since Australians don't like a lot of unnecessary complexity.

The ISO27001, it is too reactive, and crypto moves faster than the security auditors so get out ahead of it with a set of minimal expectations. A better (more proactive) approach opposed to requiring ISO27001 would be to offer automated code checks "linting" which are instantaneous and nearly-free to operate; they inspect the contracts that issue transaction instructions to make sure the 'short circuit' codes are in place (in which functional areas). The technical term for these types of systems are known as "oracles" and you might further differentiate ("word precision") your organization as a sovereign oracle providing voluntary governance controls.

Due to the nature of program code it is easy (for a technical person) to introspectively tell if a method within a contract does or does not implement a specific behavior (i.e. does it have the voluntary control instruction in it), and if the instruction preceding that includes a voluntary short-circuit (for example). The correct technical term for this is "linting" .. or "de-linting" the source contracting, like removing the lint on a piece of clothing before you wear it. While this probably seems absurd to non-technical people, the reality is putting money into a smart-contract without carefully reading the code first is a recipe for disaster, that is why we use automated tools to assess the risk, scan for backdoors, etc.

Offering and permitting organizations to utilize these capabilities should only be done as voluntary participation, such that companies can step in the release validation process for a governance contract within an organization that submits to your regulation "installs your hooks" (which are publicly observable).

This leads into a related and very important type of organizations that you maybe unfamiliar with called a Decentralized Autonomous Organizations (or DAO for short). DAOs defy categorization, and they certainly don't fit nicely into the non-custodial CASSPr paradigm. I have zero doubt that some DAO's will be nefarious hacker-hive mind criminal organizations (those already exist, and they have hundreds of millions of dollars), but I suspect many more legitimate uses will emerge in the next decade. Examples will be private family real-estate & investment trusts, schools & student organizations, churches, community organizations, and footie clubs (at least down under!). DAO's are difficult to explain conceptually but easy to use and highly efficient means for distributing money in exchange for work-input & coordination within groups. DAO's run on blockchains, so they can't be 'unplugged', and they are attractive because they obviate & securely automate a variety of small-matters (reduced headcount, especially in sensitive areas). CASSPrs as written, many DAO's would be CASSPrs and they would be unable to obtain ISO27001/SOC2 compliance – even if they could wait 6 months to a year for an audit that can easily costs hundreds of thousands of dollars in time and documentary process control. None of

those should *probably* be designated as CASSPr's.

My suggested approach to this is far more pragmatic, I would suggest beginning with the "finger" protocol for public keys to well known cryptographic validation algorithms you provide - initially ERC-20, and then expand beyond that "as needed" (ERC-20 is a ubiquitous standard, you'll cover ~99.9% of web3 with ERC-20).

Conceptually, it all begins with the finger (the protocol, used as a piece of zero-trust public text broadcast service) suite & services suitable for robotic automata and cryptographic network protocol public key distribution and ideally you should be pursuing a time-delay to minimize the instantaneous transfer of digital assets (intentional time delays with trusted intermediaries) such that rug pulls are NOT possible, or at least require some elaborate heist to break into ATO headquarters and steal your master keys in order to release the funds. The degree of difficulty to prevent both accidental loss (i.e. human custodial death) & scamming (here defined as 'intentional misrepresentation, possibly with intent to commit fraud') can be prevent by those who are aware of the ATO crypto-governance & decentralized finance services.

Your agency could therefore discover a new service based on registry lookups to discover/alert the status, and potentially contain the size of a hack/scam. This means nefarious entities can intentionally avoid targeting Australian citizens due to their national threat posture being set to "paranoid" (at least with respect to financial governance). I make a case later for this because Australia as a nation has very high safety standards in every other area food safety, ohs, etc. and I don't see any reason why crypto should be any different. Many of the things I'm talking about are best/easiest in non-custodial processes (since they don't involve people, they are deterministic), and these ideas will be foreign to Australian companies at first. Australian companies tend to be technical laggards, and this is because many lack the technical resources to properly research ideas and will wait for an idea to be presented by the technocracy 'simple as' and that is why I suggest giving the finger micro-service a go. If you take the long view, the national benefit from uniformity & automation will be substantial, Australia by nature & necessity will always be somewhat insular since the challenges facing Australians are distinct to the continent & stratified population. Don't wait a decade to implement this. The finger service I propose, literally shouldn't take more than a day or to build the most-basic version (and then it can be expanded on as necessary).

Alternative methods of "national level" problem solving you've at least got a proactive posture "paranoid with respect to rug-pull" as accreditation & registry service for Australian Fintech firms, if you want to call them CASSPrs I don't think that term adds much. It would be better to qualify by what/which types of services an organization consumes or provides (and in 99% of the use-case this can be determined with 100% accuracy by auditing a contract using a linter) - all beginning with a key exchange and requesting READ access to the contract source code (which is going to be published to the blockchain, so it's not exactly private!, it's a fair request).

Have provisions for non-provisioned non-CSSPr crypto use in addition to the entities, but it is better when approaching web3 to think of selections as a series of binary or multiple choice questions to "choose your identity" i.e. how an organization will implement it's systems such that they can be compatible (at a technical protocol level) with one or more ATO systems. When you find future gaps in your coverage decide if they are worth covering the extremely odd-use cases.

Make the companies who would exist 'outside' the ATO umbrella "out in the rain" - "no finger for them" policies as BROAD and exclusionary as possible at first. Make the CSSPr suitability requirements as narrow as possible, and provide community services on popular blockchains (in a form known as WASM & polyfills all blockchains can run the same code, so don't worry about offending any future protocol!). Non custodial multi-signatory decentralized governance, voluntarily adopting central sovereign Australian #irl oversight. (the #irl is shorthand for "in real life")

The CASSPr approach is flawed in terms of its posture/approach to traditional regulation. In my descriptions word precision - this is critical, for classifying behaviors. The nuanced differences in types of technology and people processes (i.e. Custodial vs. Non-Custodial) is a distinction that should be made at minimum *always*, and most likely I think your rules & regulations for types of organizations will likely change based on 0,1,2,3,...# of custodians, internal distinctions, in terms of both public information they must provide and private disclosures to you in terms of funds held, accounts, key-signing, contract-entity registry types etc. (using their protocol versions as references whenever possible). The nice aspect of blockchains is all of these properties are observable, especially if you enforce naming conventions for how the contracts must be written (in order to be both network & legally valid in courts).

This is why I suggest that the ATO with respect to crypto should internally strive to provide one or more IETF or code libraries/OCI WASM container interfaces or transpilable smart-contract 'source code' for decentralized 'national' organizational models. These are approved, suggested template for #include or library import into Australian corporate & other organizational smart-contract governance. I.e. "a forkable versioned reference implementation" & test-cases even at a flow control diagram level for each T/F Y/N multi-choice one or more checkbox situation of "what or who am I to the ATO". The term "forkable" means that the source code can be copied from the Internet commons, then a company can extend/hack on the source (integrate themselves into your interfaces) because the web3 provides the trust and you must only secure your own 'finger & dns' servers which should be pretty easy. Again, a person doing a rug-pull, if they must 'hack the ATO systems' first, it becomes an order of magnitude more difficult than just running a twitter bot farm.

Decide which blockchain protocols will receive which governance controls. For example the controls you can implement on IPFS are different than the controls you can implement on Ethereum. Taking a functional "how can we use this protocol" centric approach and realizing that there are lineages to these projects, and that no blockchain project starts building a blockchain entirely from scratch. The idea that a company can't implement the most basic "finger and/or DNS protocol" for voluntary registration and zero-trust key exchange says that something is dodgy out of the gate. But if a shiny new blockchain protocol or metaverse can't implement a foundational Internet public broadcast protocol originally invented in 1977 - well, it's an indicator of *something*.

Using this approach, you can properly enroll & map (into your own internal taxonomy) the entities & understand who is out there (in your records), gather usage data, verify heartbeats, even (someday) potentially do self-auditing/filing "progressive observable taxation". All these are potentially straightforward "Australian simplifications" that could be gained by the ATO designing an agency service catalog as an adopter of the technologies it seeks to regulate (at least at some symbolic level, issuing your own wallet, signing key & setting up a finger server shouldn't take an semi-competent admin more than a few hours). People can do what they want with them, public keys & wallets are cool that way! Registered charities, churches (which might give out POAP's NFT's Proof of Attendance Protocol and let those be voting on control of various church-crypto funds). This is not a problem today, but the rules as written will attempt to regulate churchs and other organizations that are incorrectly caught in the CASSPr net. Conceptually a church accepts 'tithings' (monetary donations), it might someday accept crypto tithings and issue art NFT's - so while this isn't the intention, consider the other types of organizations which may be caught & harmed by the CASSPr net.

There are so many options & tools that exist at your agencies disposal for voluntary adoption and the entire "how do we regulate this" process should functionally roll up and simplify - by providing a simple-as way for the network to trust the ATO about which entities are legit & dodgy (according to the ATO) online. The finger protocol, besides using it comically like "giving somebody the finger" or "requesting a finger" for validation are important when operating in a defacto zero-trust posture. Human custodians are easy to

deceive, so it would be better if encouraged Australian businesses to quickly adopt smart-contract controls (and in some cases, I wouldn't even certify systems which rely entirely on human custodians, there is always a way for a human to scam it, but with the proposed methods it would take collusion with your office to pull off 'some types of scams' thus removing risk from the market and increasing trust)

When you decide who is eligible to access your service catalog. Design every step in the qualification process as simply either a boolean true/false, a multiple choice list, or give us a number "steps" in a sequence to "are you subject to ATO regulations" & catalog of registration services offered.

I hope you see how this approach to naming and policy (using protocol names of services offered) would have the most impact/benefit. I suggest the wallets be a national victims recovery fund, and they can also be used to do any depository of operation taxes of 'sanctioned' national crypto-lotteries (or is that another agency?). But ultimately the AU government has a website, and so it's not impossible to think that someday many agencies will provide services on one or more metaverses. So this approach (using the protocols & terms in your own vernacular, rather than inventing your own acronyms trying to match it to your laws, creating services in network executable notation) would make more sense, since the network will be more likely to adopt them voluntarily.

Those who don't adopt them voluntarily put into the "Other" group and monitor them - don't criminalize not having a license. But offer operating licenses & service catalog. I actually quite like this aspect of the Chinese national firewall, they have a central registry system for all businesses, and every website/business that publishes anything online must have a signed ICP license for attribution & tracking. https://en.wikipedia.org/wiki/ICP_license while any company can put whatever they want on the website, a quick 'finger' or dns check could demonstrate if the claim is legitimate or not. Future wallets can incorporate these signals, and wallets could easily and quickly be configured so they 'while there are outstanding disputes/investigations/etc.' they programmatically refuse to interact (pause or reverse all transactions until the matter is resolved). By limiting the amount of money a scammer can grift from Australian people, you'll stop the nascent industry from becoming a person's "day job".

Things like that and the types of contracts that might be legal or illegal in the metaverse (i.e. how many NFT's a company can issue), and honestly there's going to be a lot of really unpleasant topics surrounding exploitation, child-safety, and other 'legal' issues which are beyond your agencies purview over which metaverses are audited/orderly regulated & voluntarily abide by AU sovereign laws & governance, speech, censorship (which should always be a matter of public record), which will ultimately cover or need to cooperate with many forms of cybersafety & national welfare.

This assumes that in the future every possible idea will be implemented, even the bad, horrible, illegal ones. By setting high voluntary safety standards you actually help Australian Web3 companies provide a safe harbor to foreign investment (with the strongest controls & action reserved for your own citizens).

Rate of change, volume of requests is an excellent measure. Too many fingers for a wallet address after it gets X 'validation requests' to your finger service places a voluntary suspension "timeout" while they verify systems aren't hacked, sort of common sense collaboration. (if your service is unreliable, and causes the smart-contract to pause, then it's a national problem, but at least there is some semblance of control). To be clear, the effect of "gating" which creates "fomo" will also probably help many AU crypto-companies.

The problem with custodial accounts is they lack these controls, the human is fundamentally non-deterministically, people can die, planes can crash, etc. but for companies who are voluntarily participating they might be eligible for a national insurance fund or something to that nature.

This covers both accidental and fraudulent actions by those companies which chose to enroll & were accepted in the ATO voluntary governance program. The goal is to have plans in advance, with mitigation for situations such as keys getting lost or compromised. So the proposal I'm giving is intended to provide one possible best-way to solve those solutions for voluntary get on a 'white list' for banks exchange (in the example of a CASSPr).

But I suggest you set the compliance bar with technical network protocols & code rather than compliance paperwork. Let companies & organizations work hard to seek and attain it, once a 'reference implementation' is published then it can be quickly transpiled into other blockchains that operate in a similar way. This is why the technical vernacular "word precision" approach is better, because the ATO is conceptually a partner & source of truth-sanity who is sitting on the same side of the table which is always better, at least in my opinion.

Instead of writing rules, you're spending more time planning technical program code 'per-se' processes which will streamline cryptocurrency & blockchain in the AU for future generations. Australia because it is so geographically stratified may actually benefit significantly more than a smaller country from widespread adoption of decentralized organizational governance. In Australia to validate a company it usually requires a plane flight, it's not like Tokyo. In terms of planning your catalog - secondary survey of specific services, should be written as simple Yes, No, we are going to do xyz services, who is eligible to register/consume them and what your expectations are.

Design your next survey as a Question, Multiple-Choice or Other (these 5 fundamental idiomatic approaches) allow for an infinite number of 'functional' self describing names since your agency would be using global protocol specifications (on those networks, such as the world-wide web 2.0, and someday web 3.0, web 3.1 ...). Roughly the syntax/speaking pattern I just described is easy to automatically translate (transpile) with 100% accuracy by encoding & decoding rules. So planning rules doesn't need to be a coder, that can be designed in flow charts using a method known as "zero-code" to create idiomatic processes.

When writing idiomatic laws (not idiotic, but idiomatic means native to the speaker), in the case of the industry you are attempting to regulate that's protocols that exist on the web today, those are service catalogs say ERC-721 (for example) with or without the three letter acronym NFT. Normally this is not how law is done, it seeks to be broad.

That is where the agency should begin it's efforts to provide the critical 'crypto' cybersecurity services (signed national custodian vaults, smart contract program libraries, etc.) and this vernacular syntax pattern will avoid you functionally need to invent new words and terms/means for classifying this - because idiomatic things are self-describing (either compositionally, or worst case using natural-language-understanding & transpilation). If you create new abstractions that are too ambiguous then it leaves uncertainty/wiggle room in interpretation & discretion.

In terms of services your agency offers, you would start with your registration page, having yes/no/maybe choices or "other" to survey which services and provide interactive help-bot-driven chat (on a decentralized protocol such as matrix, or IRC) to establish voluntary registration services for companies & persons, entity identity, public key(s) or for web-of-trust or sub-protocols as a "dead-person" [deadman] switch once per year or whatever, signatory & multi-signatory recovery agent. The deadman switch itself could be provided in a library, it's either visibly included or it's not - because it's observable, and other useful things such as dead-person switch rate-limiting, restricting outbound or inbound flows (as a safety precaution) with dead-person blessing pattern - "override knock-knock boolean switch" that enables the "drain all funds" in one go (as an example of how agencies might cooperatively desire to provide these as sovereign assurety & recovery mechanisms).

With each step in your process just have an option “Other”, and a list of protocols you support/offer (because if a project is doing something technical, i.e. on this planet), just lay it what you offer/what you provide in clean file-formats and national regulatory codebase/registration API, again as a voluntary crypto service with “large money transfer” oracle-vault-recovery service as a way to voluntarily de-risk the market and make it just a wee bit harder for the criminals claiming to subject to australian governance do rug-pulls, at least when representing they are from or associated with your agency. Agency or national bitcoin, ethereum wallets (from any recovered fines, etc. victim recovery funds, policies for disbursement). One potential advantage to the idiomatic approach is that there is no need for a human auditor or NLU (natural language understanding) transplier. I’m explaining this in technical terms that could enable giant safety nets to be installed. Simply as a “source of truth” to the network using one or more protocols directly is the most sensible next step. I’m suggesting that it is more valuable to provide tangible services to both CASSPr and NOT CASSPr (individuals, self-governing entities) other non-CASSPr forms of voluntary crypto multi-signatory control mechanisms.

Finally, I’m sort of unapologetically going to tell you to give the crypto community “the finger”, as in RFC 721 where the ATO publish one or more keys/credentials/wallet addresses on a historical protocol (Finger/name was original invented in 1977 when I was one year old. Finger is a very stable technology).

Finger guide to services as a means to start any validation/registration process. (Finger itself is a public broadcast protocol popular in the Unix community, another example of a protocol is DNS). My point is that the ATO could provide keys/public on/off switches & regulatory signals (via well established protocols, including finger) for the services it seeks to regulate.

I would suggest you offer a public finger service (quite easy) with different extensions, links, etc., and provide a lookup for entities which are allowed to get/give the finger on your behalf (this allows somebody to programmatically lookup/verify an identity that is known & valid or unknown or known-bad-actor/scam with respect to the ATO & part of a national cyberthreat safety). The ATO could provide many validation protocols, but finger is retro, easy and funny/ tech-cool way to publish your keys & address. I suggest the industry would respond well to that, even global companies might want to get or give you the finger.

I think the regulatory process program should be called “have a finger”, “here’s a finger” or something, not an acronym at all. I like finger for its high novelty low-brow idiomatic british humor value. Issue credentials, guide people to crypto-libraries & provide citizens national vaults / smart-contracts, and I would suggest the best way to get kids excited about crypto is to tell them about the finger service personally i’d go neo-modern with a url like: “finger://hello@treasury.gov.au” describing the validation services & protocols supported. finger://wallet@treasury.gov.au .. finger, wallet, again - your audience is the crypto community. The spiritual leader of ETH/Ethereum Vitalik Buterin is known for wearing unicorn pajamas when he gives presentations. The audience is young and immature and so talking about “the finger” as a broader crypo-currency & national cyber-safety policy.

Finger service (original): https://datatracker.ietf.org/doc/html/rfc742
Was obsoleted: https://datatracker.ietf.org/doc/html/rfc1288
Sub note: you can use emoji & unicode in the finger service/urls.

2. Are there alternative terms which would better capture the functions and entities outlined above?

Token Asset Issuer or Token Asset Custodian

The word secondary is incorrect.

I will recommend (in more detail) adhering more to a global industry terminology rather than creating a new Australian sub-dialect & national naming conventions. CASSPr itself is ambiguously vague and simply gives it a catchy non-acronym “very long sequences”. As a national organization if the ATO is keen to be seen as innovative you might try to skip the acronym. If you want to use ideas to represent these - don’t use one-way non-reversible acronyms like CASSPr.

In addition to “finger”, I would also suggest one or more #include <“//git@github.com/au-treasury/ /”>; library projects (or use a kangaroo or whatever, but just symbolic projects) or something equivalently in technical library style is just one layer of abstraction, provided national crypto services. Australia is effectively a technocracy, so adopting new/better ways should be more intuitive & easier - less red tape by more “passing build tests”. By styling your rules in an “idiomatic” codification of protocol services offered in the catalog/source-code repository with good “how to” implement guides seems like the correct approach to me. I hope that you consider the significant benefits of this possible approach in terms of how many incredibly useful services the ATO can provide in the forms of validation & insurance underwriting/compliance role and stored in a git version. The crypto regulations from version 1 could simply reference the git hash, and regulate the industry through GIT source code version control & collaboration (*it will be more familiar, and build skills in the tool so that you can better understand/regulate it).

The entire process/system and simultaneously differentiating situations which Is-CASSPr & Is-Not-CASSPr also needs to be revisited. Several other points along the way which hopefully advance & inform your own ideas on what is possible.

An example of idiomatic coding might be using a ! at the beginning of a word to indicate a “NOT” as a preamble to translate Australian national code to blockchain executable code. Blockchain wasm program code is a polyglot language ‘universal tongue’ of languages. WASM facilitates a transpilation (conversion from one language to another, with digital fidelity) and a feature known as polyfill that ensures forward and backward compatibility.

If you are going to write laws about crypto, it should be done in a mechanism where the registration processes filing etc. might be stored on the website for public safety. Your target output format should be functional WASM and cryptographic identity / key validation.

Also - and this is a big one – the CASSPr term should definitely have the term “Custodian” for rules which describe processes that involve humans holding keys. I will explain later that non-custodial entities are behind (more complex, took longer to build) so the firms you are regulating today aren’t how the firms of tomorrow will behave. So considering the term Custodian (and deriving more words, to describe roles, how people receive/spend tokens/money earn bonuses, what is gambling, what is fraud, etc) and at least some word for Other-non-custodial entities - they can ONLY be regulated using the tools that define their boxes (which is the blockchain protocols themselves, they inherently limit what a smart-contract can do)

When agencies add more words and ultimately have a flow chart and specifically for (at least in the case of smart contracts) writing said regulations in an idiomatic natural language coding style (to simplify the national code) - or even better solidity, but one or more services/libraries that can be “included”. Even if the preamble is traditional AU-legalese, it is straightforward in our modern or near-future era to have NLU (Natural Language Understanding), and the more closely this reflects the industry standards as regulatory code, that is also potentially planned for as executable and therefore easier to adopt, because the terms are less ambiguous. It is important to realize that 100% of the crypto smart-contracts are designed NOT to require a custodian at all (self-governance). This is one example of a non-custodial entity and so for word precision I might suggest that !CSSPR would be said or read as “not casper”, because 5 letter acronyms the NCSSPR doesn’t sound as nice.

Additionally I want to point out the opportunity for potentially carving out registration criteria early for political-jargon regulatory purposes such as “green crypto” (Proof of Stake, energy efficient) vs. “black crypto” (Proof of Work, power consuming, grid breaking & potentially fire starting) how you might regulate those (or even categorize/audit/validate) which companies are for example running on green energy vs causing fires by taxing the grid - especially as humanity faces an uncertain climate - surely it is conceivable that someday such distinction may want to be made earlier. Which protocols or entities are KNOWN to be insecure, etc. which (if any) service outages, other national news, twitter, other & messages, phone numbers, email addresses, etc. are all suitable topics to include in a finger.

3. Is the above definition of crypto asset precise and appropriate? If not, please provide alternative suggestions or amendments.

Incomplete.

The term Ownership is incorrect, it is Controlled by, or Assigned to a Wallet

Please use specific protocol numbers ERC-20, ERC-721, ERC-1155

4. Do you agree with the proposal that one definition for crypto assets be developed to apply across all Australian regulatory frameworks?

Yes, having one regulatory framework for everything makes sense.

5. Should CASSPrs who provide services for all types of crypto assets be included in the licencing regime, or should specific types of crypto assets be carved out (e.g. NFTs)?

It is better if you explicitly define the types of tokens, based on their protocol numbers rather than speak generally about them, with guidance for new situations.
The lack of word precision with regard to generalizations such as “NFTs” should be ERC-721 can be implemented differently under different proposals - so ultimately while I support specific & exact examples (with protocol numbers), I do not support any proposal which uses generic terms and generic 3 letter acronyms such as NFT. Break down bigger concepts such as i.e. “is it a crime” and include validation services to audit contracts for compliance using an automated syntax linter. (A linter is a debugging tool that can also enforce formatting, i.e. “checking for lint” on your clothing, it’s an automated assurance tool, and quite easy to do). ATO cyber-services Linting a contract/module that (for example), a voluntary validation step that might happen during the release process, to ensure (for example) there is a voluntary ‘known’ regulatory backdoor & minimal audit service.

Auditing code (even idiomatic code), can be put through an *automated* syntax checker. These can be legally trained natural-language understanding artificially intelligent transformers, or better yet, just write the original in pseudo code.

Smart contract code is compiled ultimately into a form known as an ABI, Application Binary Interface which itself can run WASM. If a network can support smart contracts AND the network supports ABI AND the network supports WASM then the ATO rules & regulations will “compile” and run natively as a library in a service catalog.

The service catalog should include anti-rug-pull inspection/controller ‘safety light’ network-“oracle” that can deterministically influence the outcome, delay, or properties of transactions matching a filter or in control of a website that allows/denys actions, and having the inspection/assurance of oracle code [not oracle the IT company, oracle as in ‘the all knowing eye’]. I.e. “before the funds can leave the organizational wallet, a would-be rug-puller would need to appear at the ATO office and get it signed for” sort of services that just take the fun out of white collar crime, but enable legitimately useful and necessary “nuclear” options for liquidation & recovery, or voluntary network short-circuits and/or extraordinary-recovery short-period time-travel within a blockchain services.

6. Do you see these policy objectives as appropriate?

I think these use an Australian parlance & vernacular that is technically incorrect and will make the policy objectives ambiguous.

7. Are there policy objectives that should be expanded on, or others that should be included?

Yes, I will cover these later.

The short answer is - according to your definition any company or organization that uses crypto currencies in any capacity is a CASSPr. I will explain momentarily while this is probably bad/dangerous.

8. Do you agree with the proposed scope detailed above?

No, it is overly broad.

9. Should CASSPrs that engage with any crypto assets be required to be licenced, or should the requirement be specific to subsets of crypto assets? For example, how should the regime treat non-fungible token (NFT) platforms?

In some circumstances yes, but not in all circumstances - not just NFT’s, because ERC 1155 is NFT + Coins, and that is perhaps most useful to apply to video games, and those can have ERC721 (NFT’s) and ERC20 coins inside the contract.

10. How do we best minimise regulatory duplication and ensure that as far as possible CASSPrs are not simultaneously subject to other regulatory regimes (e.g. in financial services)?

Declarations of organization type - intent & purpose.

11. Are the proposed obligations appropriate? Are there any others that ought to apply?

No, I think they are confusing and non-specific such that they clarify rules for fin-tech companies and could reasonably stifle & retard other forms of technical innovation within Australia.

12. Should there be a ban on CASSPrs airdropping crypto assets through the services they provide?

No, this is stupid. Airdropping is not synonymous with scam, there are legitimate reasons to use Airdrops (and lots of illegitimate reasons too)

13. Should there be a ban on not providing advice which takes into account a person's personal circumstances in respect of crypto assets available on a licensee's platform or service? That is, should the CASSPrs be prohibited from influencing a person in a manner which would constitute the provision of personal advice if it were in respect of a financial product (instead of a crypto asset)?

A ban on not providing is a 'requirement' to provide advice.

Crypto assets are a form of financial instrument requiring their own disclosures, some which may be very technical.

CASSPrs which are offering investments, specifically PUBLICALLY offering investments on radio, television, or online advertising should be held to higher standards - specifically a requirement to register with the ATO and for the ATO to maintain and publish a list of benevolent and malevolent actors that can be used as a allow/deny access list by banking apps or national wallet/exchange providers.
I have suggestions for how to do this later.

14. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

I am definitely a CASSPr simply because I would get paid in coins, via a DAO, and I shouldn't be subject to these requirements, nor would the DAO be subject.

The cost will be variable depending on how simplified the final process can be made.

It might be more appropriate to be transaction volume based and allow smaller community organizations to simply stay under the radar for things like crypto payments at a sausage sizzle.

17. Do you support this approach instead of the proposed licensing regime? If you do support a voluntary code of conduct, should they be enforceable by an external dispute resolution body? Are the principles outlined in the codes above appropriate for adoption in Australia?

Yes, absolutely provided participation is voluntary and there is a way to distinguish who is telling the truth about participation & ethics.

18. If you are a CASSPr, what do you estimate the cost and benefits of implementing this proposal would be? Please quantify monetary amounts where possible to aid the regulatory impact assessment process.

It depends on the nature of the CASSPr, their goals, many of these are fixed costs that are best suited to AU fin-tech companies, the would be sufficiently onerous for small privately held non-fintech companies that I would consider never launching some types of projects in Australia - this could retard the national adoption of blockchains and digital currency.

19. Are there any proposed obligations that are not appropriate in relation to the custody of crypto assets?

I think it's obvious I have significant issues with how the mechanisms are described, especially by the next section. I will explain at the bottom in a longer form with some narrative.

20. Are there any additional obligations that need to be imposed in relation to the custody of crypto assets that are not identified above?

The idea that this section doesn't have the word "multi-sig" or multi-signature, or specifically outline methods basically means that it's far too open for interpretation. Especially section (8) will be onerous for many types of smaller CASSPrs. I offer both criticism and broad solutions later.

21. There are no specific domestic location requirements for custodians. Do you think this is something that needs to be mandated? If so, what would this requirement consist of?

Absolutely not. Generally custodians are the weakest part of the entire system and the easiest to attack.

22. Are the principles detailed above sufficient to appropriately safekeep client crypto assets?

Absolutely not. They are inexplicit, the standards of care can be widely interpreted.

23. Should further standards be prescribed? If so, please provide details

Yes, explicit terms rather than ambiguous laws. Minimal standards should take into account the terms such as & kill-switches.

24. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

The cost of an ISO27001 audit is going to be $10,000 (minimum, annually or quarterly) plus significant time & resources to setup the systems & paper work and ongoing obligations.

25. Is an industry self-regulatory model appropriate for custodians of crypto assets in Australia?

No, probably not in all circumstances. Self-regulation creates asymmetric knowledge and can be difficult for the consumer to distinguish between differences.

26. Are there clear examples that demonstrate the appropriateness, or lack thereof, a self-regulatory regime?

Yes, the self-regulatory regime will generally try to be broad and inclusive out of necessity. In reality what consumers need is a regulator who can provide some level of certainty with regard to benevolent and malevolent actors (which a self policing community will NOT do - because bad actors lie)

27. Is there a failure with the current self-regulatory model being used by industry, and could this be improved?

There will always be failures, that is unavoidable. A better question would be what will the ratio of failures to success be, related to consumer confidence in one regulatory model vs. the other.

28. If you are a CASSPr, what do you estimate the cost of implementing this proposal to be?

If I'm starting a fintech company this is very reasonable, for everything else (i.e. small non-profit, community orgs, footy clubs, issuing NFT', etc.) this would be non-viable & exceed the budget. Extremely unreasonably onerous.

This is why I made the case for automated linting, because the cost of compliance (for organizations which choose the non-custodial, automated control much better, but still collaborate as a way to protect your citizens!) .. this effectively means that once a contract is on your code, the contract can't be updated to remove your code without permission (unless the entire network was to reverse an invalid decision).

The blockchain networks should probably be administered by the UN or WHO or international body, but there is no reason why a large company using a blockchain might have multiple "international" assistive or regulatory safety controls.

Word Precision vs. “Australian” Word Compression

I wish to draw some attention to issues I had while reading the entirety of the paper. I point out several biases I’ve seen, emerge in this paper and more broadly within the Australian blockchain community. I realize I’m approaching this like an American technologist and you’re likely to ignore me and this is simply my point of view, but I lack the words in Australian to properly articulate this.

Absolutely, there are many wonderful and frustrating things about being from Australia - but as an outsider there are several biases that felt apparent to me. “Word Compression”

Page 14. This regime would not apply to decentralized platforms or protocols.

This is one of two occasions the word “decentralized” (or I, as a recent emigrant from the USA might say “decentralized”) appears in the consultation document. Decentralized appears *ONLY* twice. Again, I will stress adding words for word precision during your planning process and now I hope to bring to your attention a bias in decision making that could inadvertently put Australia a skew. Another point of differentiation beyond custodian is DECENTRALIZED vs CENTRALIZED blockchain ledgers in terms of word precision. They have very different governance models, and the advisory documents to prefer the centralized ‘custodial’ approach, so there actually 3 classifications (custodial decentralized, non-custodial decentralized, custodial centralized), and this document explores only 1, and the 1 it explores is the least common *outside* of Australia i.e. ‘which globally, is mostly crypto-anarchy type persons) but most popular inside of Australia, ironically is custodial centralized in a survey of companies using blockchain to solve problems in Australia.

I have been following the progress of Australian crypto-blockchain community projects, especially in agriculture. Australia has a population that is stratified across a large area and so decentralized governance technologies (such as those which would hold digital assets) are extremely well suited to AU but presently unused in a variety of capacities due to Australia often being a technology laggard.

Community DAO organizations are widely popular in my home-state of California. (To be clear, I’m now in Melbourne, VIC with my Australian wife, and I am a cybersecurity & blockchain developer so I have a stake in this).

Blockchain based organizations such as DAO’s are exceptional tools for operating distributed communities (such as selling NFT’s for memberships to a charity club). DAO’s are suitable for a wide variety of organizations ex.: a local charity, footy club, a church, a coffee shop with multiple partners, a

research development corporation, a real-estate investment trust/partnership, or decentralized global corporation. Each organization has different needs and rationale for choosing a DAO blockchain-crypto-governance structure. I hope that suitable distinctions are made for LLC limited-partnership personal or family office DAO's, smart-contract trusts that may hold assets, and have no people in a marketing department. The document seems to neglect this aspect of blockchain technology and then proposes rules which are possible-but-absurd / irrelevant after the organizational contract is live.

https://blog.ethereum.org/2015/12/04/ethereum-in-practice-part-2-how-to-build-a-better-democracy-in-under-a-100-lines-of-code/

I believe the present proposed guidance by the ATO will have a chilling effect on the smaller types of organizations who could greatly benefit from internal-custodial structures by adding onerous complexity such as ISO27001 audit requirements.

I will stress increased "word precision" and then translating those conceptually to functional symbols & naming conventions if you are going to make them necessarily complicated to implement using your approach. Don't create another dialect.

My suggested approach is to use an idiomatic syntax - design or utilize an existing program code friendly lexicon as a way to draw/transpile your technical laws, using symbols for checkpoints in the regulatory process "to summarize", in flow diagrams to illustrate.

Flow diagrams as the ones suggested can be automatically (in a build pipeline) translatable precisely by referencing or creating various existing technical-standards IETF "Internet Engineering Task Force" style implementable protocols, known papers. Using this vernacular & reference for technical industry regulation this is one place I would start when writing the actual technical regulations/specifications of how your agency should approach regulating technology.

Ultimately I suppose the role of the ATO is to provide validation that a specific URL, domain, entity is in compliance, with respect to your internal reporting systems, and which aspects or registration type(s) they are filing with you. Don't write a law, write a protocol, then write the law that says see the protocol (& reference libraries).

The agency aspects of regulatory compliance, and you as a national agency provide signed revocable keys to the custodians and monitor asset transfer optionally provide crypto-oracle supervision & crypto-fraud prevention.

There are many ways to approach this, all are valid and better than the proposed method. If you want to regulate an industry, your industry should step up to the challenge, meet them halfway here. Many of your present and future national crypto-aspirations can be quashed by overly broad legislation that only makes rules criminal custodians won't follow. One of the reasons crypto is actually awesome/humanity, is that it isn't just an Australian thing.

My approach suggests simplified, registration file types names & "large group" emoji or custom AU font/character set & text-based block diagrams or even emoji or aboriginal patterns character-sets. The

symbolic approach is one of the reasons why the Chinese coders are able to crack out more code than the Australians using the western 26.

If you're going to make laws about technology I encourage your organization to do it in style, rather than acronyms - style in my opinion would be technical specifications, this approach will also be better & more precise 'faster to implement' for the global community & Australian nation.

Provided there is other forms of crypto assets which are managed or issued by entities which are distinctly UnCASSPr or NotCASSPr, and then you put up a registration application and see who is voluntarily going to integrate your validation & oversight in it's most benign form which is a validation the URL & project is in your database.

are also outlined because any attempt to regulate an industry early tends to bias the first arrivers in an industry - in this case it was the crypto-exchange that are being regulated. However the language is sufficiently broad that it could inadvertently catch a lot of potential 'other techs' that aren't widely popular yet, at least not widely popular or well known in Australia yet 'emerging tech' that would also be classified by CASSPr.

When I talk about CASSPrs I do not see a fin-tech company trying to sell ico-coins in lieu of shares to investors, I see a small community group or a Makerspace(s) using distributed governance to manage membership, probably in a chat group where they also coordinate a sausage sizzle at the park. Using a DAO for a governance model as a treasury with an automated comptroller is ideal, especially for scheduled payments, and offering members complete transparency. The rules for smart-contracts are explicit, and these are never going to be well served by generalized laws. Modern software can be designed to be compositionally idiomatic (meaning easy to read) and it is better if you do not create a separate legal-vernacular (or at least explicitly cite protocol numbers as examples).

There are many extremely useful & high-utility applications/reasons to use smart-contracts as instruments. There is potential for every single business across Australia for holding & issuing crypto derivatives, insurance, escrows, paying international employees, and all numbers of silliness. I hope to persuade you to consider special considerations or the impacts on laws and the impact they might have on the smallest organizations who may someday aspire to wield these mighty tools. These are, respectfully, my suggestions for your overall strategy and how it should inform your laws.

Please allow me this short bit of narrative. I would like to thank you for reading so far. I quite enjoy the civil, polite & overall high quality of life Australia affords its citizens (especially the lack of gun violence, ranked choice voting). As a foreigner I struggle with the Australian spoken vernacular for technical terms which are often abbreviated, shortened, or otherwise lacking sufficient detail to distinguish differences from context. Lacking sufficient "word precision" is a frequent contributor to communication errors & in my opinion contributes greatly to Australian way of thinking. Lacking word-precision causes important nuanced distinctions between two seemingly superficially equivalent "similar", but also distinctly different concepts to become blurred and synaptically fused as indistinguishable for most Australians when speaking in the native idioms. The term I acquired in Thailand to describe this is "same-same, but different", meaning it's functionally similar, but not identical, and don't let the differences bother you (on the street in Bangkok nobody cares if it's a fake Rolex, only that it functionally is ticking and looks like a Rolex, because nobody can tell the real from the fake). The Australian vernacular equivalent is word-compression. With Aussie word-compression it would reduce even further to "same-same", or "same-as" dropping the "but different". At least that is how I think the Australian language shortening

frequently works with other words & phrases, so it is entirely possible that I misread parts of your paper and there is some implicit unspoken vocabulary that fills in the words that I haven't gotten yet. US English and Australian are something completely different entirely so I'm trying to communicate things that I don't know the word for in Australian due to my limited vocabulary and say the wrong thing.

Same-same but different, vs Same-same, when summarized will incorrectly appear identical to the neophyte. There is no clear way to tell the difference between two things especially when compared in their abbreviated form "same-as", the difference becomes lost. I think Australians don't realize how frequently this happens, at least in my observations, where meaning is lost or fundamentally changed during normal Australian life. There is only one choice, they didn't even know other possibilities exist creating a blind-spot bias for the Australian. I've got no problem with Aussie "word-compression", except the "there's only one choice, it's all same-as" becomes dangerous if codified into a generalized law. Word precision is important especially in science & technology, & computer systems engineering because without word precision our specifications are useless.

Australian as a language, a fundamental part of the national identity is known to be a shortened lazy version of English. So now it is with this concept of US-english "word precision" vs. AU-english "word compression" - I can say that I reviewed your consultancy paper and found it to be significantly ambiguous, for me as a person who evaluates the pragmatic points of implementations. Not any specific part, beyond conceptually categorizing many small ideas into generalized large ideas. I felt there was a tendency toward what I am going to refer to the Australian blockchain bias & more generally security oriented fin-tech companies (which absolutely makes sense given the ATO's role)

So when I read the paper it seems to assume that mostly-only fin-tech organizations will use blockchain and we'll pretend that smart-contracts hold digital assets too. The document seemed to be pro-custodial (human custodians), and so that is how it is oriented. That assumption is very flawed in my opinion, incorrect by omission. But somehow when it is written in Australian it all seems quaint and makes sense because it's so simple (hint: it isn't that simple, the implementation details are nuanced & complex), because this paper is only written for a specific audience (fin-tech) type of company. I will attempt to explain why I think this happens, what you can do about it. To do that I need to pull on the sweater thread for a bit and I certainly don't mean any offense by it - I really struggle finding the right words to illustrate this point.

Crypto-coins & blockchains are a diverse tapestry of ideas and technologies that are competing in cyberspace for visibility and dominance. If you want to limit the Australian market to only these types of companies it will limit consumer choice. There needs to be a way to distinguish "at home" regulated entities from International non-regulated entities. Australians won't know much about them, or there will be some same-as version but it's not same-as, it's just Australian and it won't be until people travel abroad that they see the self-driving uber-taxis & cardless payment systems and wonder "gee, why don't we have that xyz service in Australia?" Sometimes this is good because it makes Australia a bit more self-reliant, but also many of the technologies can take years or longer (or never) arrive in Australia.

The ATO, today, I acknowledge what you wrote - perhaps this is probably best for TODAY with what you know. At least today it's true because of who/how Australian's do things in their own way and will keep doing things that way, same-as, because there is often little choice or distinction. I therefore encourage the ATO to consider your national contribution within your guidelines to be overly precise and specific - to incorporate additional word-precision with guidance in a more technical & protocol centric way,

idealistically this would be program code for compliance & review, even if it is fee based, the stamp of approval is worth the price of admission for the company. To perhaps break the same-as and outline or even innovate some regional vocabulary for describing and classifying these companies and organizational structures & entities as legitimate/regulated, legitimate/un-regulated, unknown, definitely-illegitimate. I think all of these are ideas you should explore. If somebody needs a waiver that would be the process, but lay out at least one clear path that is okay for possible scenarios (even if you use fictional companies).

So within the consultancy paper - there is a lot of word-compression, not enough word-precision, resulting in a conclusion of same-same, when in reality they are same-same but also different. Drawing the differences between the distinctions in the technology because it is necessary (requisite) to understand why one approach is (for example) safer than another. I appreciate you don't think that's your role, but also actually if you're the regulator then YES, that is your role. Allowing and designating the regulated 'safer' vs. self-regulated 'industry org. best practices' vs. 'other' – also can I start my own Industry Organization and set my own standards?

Companies should definitely be required to attest to their cybersecurity posture and I can assure you that ISO27001 & SOC2 are both comically laborious and inadequate in a wide plurality of situations. (I say this as an engineer familiar with the process). Both of those are also really expensive, again there are situations where these steps are needed and other situations where what is needed is a really simple-as way to just get it done easily & properly with minimal hassle (if you ask me, that's the Australian way).

The vernacular used in the consultation paper that I hope will be clarified, and also broadly lacks awareness or mention various forms of technological controls (such as blockchain oracles, programmatic audit controls) - these are examples of words I expected to see. I think I was expecting, given the other dystopian video surveillance and whatnot that the ATO were perhaps planning to build a transaction auditing Oracle (national transaction controller) to accelerate & simplify blockchain adoption.

I believe the ATO should either operate its own AU Oracle or have a university sponsor one and not leave the job up to a series of competitive companies, just have one national system for crypto-compliance & safety - that is in my opinion, the national benefit would be immense, that is the simple-as solution and obviate a lot of the security controls, focusing on the simplicity and ease with which digital transactions can be made (at least for national applications). In some circles of friends (those abroad, especially the crypto-anarchist types) what I just proposed to you would melt their minds. But the reality is the dark market version of crypto will always exist, but most Australians won't want to use that one if they have access to a free voluntary crypto-safety & regulatory system - it's one of those ideas I'd expect to see in a European country in the next decade. I think any law that doesn't adequately describe the operation of a smart-contract is missing a big part of crypto-asset controls.

Further that the generation 2 blockchains with smart contracts (such as the Ethereum Virtual machine) be distinguished from 1st generation coin is a proof only like bitcoin. Greater distinction will bring clarity since you can't treat all these things as the same when they aren't at all. Crypto, at least for the next decade will probably continue to outpace the regulation, the best way you can help the industry is to provide a national approach for businesses that everybody (not just fin-tech companies) can rally behind.

The consultation document seems (to me) to prefer and placing emphasis on human custodial roles & manual audits in governance. This is absolutely the most laborious and in-my-opinion worst-security way to implement these systems (relying on humans in the process, they can be phished, smishing,

cyber-attacked). I'm a systems engineer, so I usually believe those systems that depend on humans are the slowest, most expensive and least reliable, prone to fraud & corruption. I advocate for fully-automated 'zero-touch' patterns. If you agree that humans can be cheats, crooks, swindlers, or even that their minds can fail and their bodies are mortal then why would you ever want to put them in charge of money. So I don't want to be disrespectful when I say - you are aware that computer programs, contracts on the blockchain can hold crypto-assets in addition to individual people. This will be far more common in the rest of the world, but it might be less common in Australia if you don't think about the rules, process, etc. for when/how this is okay and outline at least one correct 'reference' way of implementing systems that Australian startups/coders can use as a reference.

From a national perspective you should be encouraging people to use smart-contracts faster adoption is better, make it easier, make it safer so more everyday Aussies can use it with no worries, mate. This should be the national strategy in my opinion. To say that smart-contract governance-DAO's are transformative for streamlining businesses and making them more efficient is an understatement, they are only slightly less significant than AI & bio-engineering in terms of impact to countries over the next decade (I expect, seeing the potential for impact).

So while Australia is a free-market capitalist society - there is a public desire to build your own version of utopia in the Southern Hemisphere. So I am proposing national open-source crypto projects, written in code that are suitable and step by step instructions on how to use these tools for Australian businesses (not just fin-tech "CASSPrs" & fiat-currency exchanges). Not exactly a kit how to start your own fin-tech, but a good example would be a non-custodial footy club with DAO governance using native crypto automated comptroller & voting - what is okay, what is NOT okay. That's the 'simple-as' diagram/guidance we need, somebody providing oversight to the crypto-non-profits about how the money is being spent, things like that!

Society I suppose tends to keep doing what already works since introducing new ideas to people stratified across such a big space with so few people is probably really hard. Just because footy clubs aren't using blockchains YET it doesn't mean they won't someday, unless the law makes that onerous, then they definitely won't.

This is one of the reasons why blockchain should be a more visible project in Australia, i.e. the diggers ability to form cyber-communities, it's a very sociable culture – so leveraging the national cyber-infrastructure using these decentralized organizations effectively nullifies the distances separating people and even the reach across oceans to other countries is marginalized. This helps everybody when we all use the same Internet (and vocabulary). In other words, when I read the proposal I see an Australian fin-tech selection bias (no shocker, you're the ATO). The rules proposed are written with a selection biased of strictly mostly-traditional fin-techs I worry the ATO will retard or eliminate the adoption of blockchain assets in non-fintech community-organizational scenarios.

I was surprised that I didn't see anything about land ownership in crypto. I recognize that request is probably better suited for a different department in the technocracy. Is there a national Crypto Research Development Corporation, is such an organization planned? That is probably in my opinion the correct vehicle to study this given what very little I know about your government organizational structure.

I say this to explain that well written regulatory blockchain rules & guidance is perhaps the best method to tap global talent & bring additional innovative methods to Australia, and again these are projects which it's

probable other countries may want to collaborate on the idea of a crypto-safe harbor in Australia, or a group of countries offering a crypto-safe harbor.

Australia is a small market nationally by population, something like 12th globally by GDP - but blockchain is literally the future of all global currencies and there is both a moment and place to recognize that Australia is either going to be nationally “doing it’s own thing” (by itself, with the rest of the world doing something else) or internationally this is a great moment in human history for Australia to lead, and try to make itself the safest place in the world for any trustworthy well regulated blockchain company to operate. “The Australian standard” with regard to highest levels of certification for large fin-techs should be extremely onerous and difficult to obtain, and so there are different goals in this regard but BOTH organizations might be classified as CASSPr’s.

I’ve been going on about word-precision & word-compression. I do not want to see Australian crypto be retarded accidentally in it’s early growth by lack of word-precision, creating only one best way that works only for the group of persons the law was written for (yes, again - I realize this is Australian and it seems that is how things may have been done historically here). The governance to comply with AU rules will be more onerous simply because there are fewer potential customers to amortize the costs per citizen and support many when it is better for many in the country to rally behind few proven / approved mechanisms that are regarded as trustworthy (able to be trusted) this will result in better & faster consumer adoption.

In terms of remediation the way to solve this is to create a situation where more global citizens want to use Australian regulated blockchains & smart-contracts. I totally respect that Australian doesn’t want to be the decentralized crypto-anarchy unregulated market running on bitcoin like some South American country, so why not use the regulatory framework to encourage & direct certain types of national policies related more broadly to smart-contracts with government supplied currency controls (In programming parlance we might say #include <australia/crypto.sol>;) and that just overwrites the send/receive fund function hooks in the smart-contract language (solidity, in this example) and you have your own nationally versioned audit controls “Oracle” and the ATO tells all AU companies to use that OR be subject to the other set of highly onerous rules. This is my high-level solution to the problem I have been describing.

The term in programming is called “overloading” a function with a new definition. That is my definition of a crypto-safe harbor and as a US person I’d be inclined to sell digital e-citizenship for international people wanting to sign up for it if you wanted to really spread out the development costs across the rest of the planet. I believe this idea could be more popular than you might think (not with crypto-anarchists, but every-day Australians), and of course the real crypto-anarchy people are going to lose their minds but you’ll accelerate your national development of smart-contracts by having rules that are broad enough to cover everything, with some guidance for things it explicitly shouldn’t cover. The present discussion about these technologies focuses too much on the financial offers, and seems to miss the utility of using smart contracts to orchestrate financial transactions because most Australians businesses don’t do that *yet* (and they might never, if they all have to get ISO27001 audits to use crypto-currencies)

In computers all the languages are presently converging with the ability to compile any language into a single bytecode known as web-assembler (WASM). WASM is one version that runs on ever machine, in every popular language that a person would reasonably consider writing a payment app in (WASM is new-ish, but already enjoys ubiquitous compatibility). And I want to be clear in suggesting that WASM libraries as an ATO ERC20 auditor, is appropriate for business and organizational transactions, banking apps, any national way of sending or receiving crypto-currency for tax/accounting purposes). The term for this type of system that controls the transactions is called a Crypto Oracle and then you have the (present) onerous rules for organizations that can’t (for some reason). Create a national whitelist of

wallets that are whitelisted i.e. ‘re registered with the ATO’ for verification/in-good-standing, be able to shut down scams, intercept & recover funds, etc. these scenarios can all be adequately addressed using this approach.

If the ATO Crypto division were to consider providing an Open Source libraries describing one-or-more mechanisms how to store Blockchain & store assets, both for fin-tech and non-fintech organizations. Ultimately clear guidance & examples could be transformative to the economy, and this would be specially true if it were possible to write the law in an Australian idiomatic program code/vernacular that could simply be downloaded, included and compiled in to ensure compliance is ‘managed’ - this would likely cover 80% or more of ‘easy-as’ use cases and just let that be the template for the exception/route & provide acceptable use cases and let the law simply reference that mechanism, the Oracle route.

These types of projects that could easily be done in conjunction with a school or as specialiced Crypto Research Development Organization (similar to the other Australian research development organization) and I would specifically like to mention/suggest Oleksii (Alexei) Konaschevych who is a professor at RMIT specializing in Blockchain & Digital Governance. The Australian Institute of Digital Transformation as a person who might be good to lead such a project, I enjoy his youtube channel and I hope whoever is writing the final version of the law has thoroughly reviewed his material and comments.

The Oracle aspect let’s call that Project #1, and Project #2 is an and ideally a forkable ‘ready to compile’ DAO CASSPr-but-not-CASSPr charter for footy clubs, community orgs, investments, trusts etc. with a non-custodial automated comptroller that is easy-as to setup (and let them using the Oracle), so Project #1 (Oracle) makes Project #2 (Crypto-Assets) safe[r], but at least at that point these projects have some symmetry, they can be insurable or nationally covered for some sovereign amount, not for large amounts but for small amounts.

These applications, for projects, trusts for parks, etc. will promote & simplify the adoption by providing smart-contract templates. I encourage the ATO Crypto group to consider not only incorporating these ideas into your rules, but also sponsoring national hackathons or similar as a way to encourage students & more Australians to actually embrace the myriad of possible use cases including national crypto ERC-20 identities, employee voting, bonus or revenue sharing, and of course corporate governance.

Consumers need regulators to simplify and make things easier & safer, and bring order to the chaos – adding more ambiguous technically inexplicit regulations does not do that. Australia enjoys a well deserved global reputation that is respected for its high standards & ethics.

A well written policy, with safeguards (‘guard rails’, such as an Oracle) may attract international companies to Australian shores as a way to demonstrate the high-standards of crypto-projects. The laws must be written to encourage more/better automated controls rather than human audit protections. The human custodial controls are easier for non-crypto people to understand, but the human requirement is continuously fallible, whereas automated roles, ultimately any bugs will be found and eliminated. Humans in any custodial process are always subject to some dodgy activity by the individual, or group, whereas an automated non-custodial system is something else entirely.

So the legal guidance should be written to prefer or at least from a word-precision perspective distinguish between audit mechanisms for custodial vs. non-custodial organizations.

There would be benefits to organizations started abroad to participate in a well-regulated safe-harbor of (mostly) honest actors that is onerous and hostile to nefarious actors. Australia, if it had slightly more progressive rules, might create a scenario similar to Ireland, which enjoyed many large corporations putting their global HQ there and that act ultimately creating a technological innovation hub in Dublin.

Using that lens "of what is possible" - my opinion is the proposed guidelines fall short, they are written in a conservative and not-especially technically innovative way, what I would describe as "traditional-fintech in crypto-clothing" - that is what I worry the future of AU fintech is. The AU equivalent will be insular, with mostly AU fintech (not much, but some global fintech). AU fintech will lack the regulatory word-precision for consumers to distinguish between trustworthy & nefarious rug-pull actors. The limited Global fintech will enjoy a mostly closed market, and Australian consumers will have limited choices. I can therefore only conclude as written, the proposed guidelines are unlikely to usher in a blockchain technological renaissance & mass adoption I would like to see happen in Australia, but perhaps that is most desirable.

I do not believe that was the intention of the consultation paper, but I proffer that the paper & rules as written is too biased toward large 'securities oriented' financial companies which in the present day consist of 99.9% of the market, but that will (through selection bias) eliminate the growth of the other less-profit more-altruistic types of clubs & community organizations (smart-contract applications) that are also possible.

So I am writing here to advocate for those other applications of decentralized blockchains and at the same time wish to express that I believe these recommendations will make AU crypto-companies more successful globally.

I cite the Australian Therapeutic Goods Administration which requires double blind, efficy based, claims compared to my home of the US which allows anybody to slap a label on a bottle and sell snake oil, the same should be true for crypto, the word precision when mandated by a regulatory body such as the ATO is significant.

Having a process whereby companies or organizations are able to identify and distinguish their using simplified technical jargon - such as "green-crypto" (for energy efficiency, PoS) vs "black-crypto" PoW crypto is only one example of a way to categorize & differentiate blockchain applications the ATO might use to identify crypto-assets or tax-classifications. The word precision that distinguishes different types of financial instruments must also be applied strictly and consistently to blockchain companies, stressing how using more word precision at this stage in your national regulatory planning process can streamline & simplify future needs to encourage, inform & support various national policies such as usage of energy.

One example of already improper (globally deviant) word precision of Australian word precision vs word compression I would like to highlight specifically.

It appears that many/most Australians blockchain applications operate on centralized ledger blockchains. Australians as a society are aligned to a central authority so it's not at all surprising this pattern was chosen - that is not my criticism, the centralized pattern is fine however it is a bias you should also be keenly aware of (and ideally compensating for).

Again to explicitly call out the word-compression, in Australian, the word blockchain, when referring to a domestic application is more often centralized, such as the AEMO energy blockchain, a blockchain most often means "centralized ledger", whereas globally it's a a blockchain is synonymous with a decentralized ledger. This makes Australian-English sound dumb, because "Australian blockchains" are usually administered by single centralized operators (which can fall over) rather than decentralized blockchains which are run by networks and millions of operators. In this capacity, your conclusions are disturbing because they are prone for centralized blockchains - which is going to leave Australia at least a bit confused (nationally, if up means down and down means up) but also more practically with inferior technology.

This does not explicitly favor one approach over the other, as a way to provide simplified guidance to Australian consumers & commercial investors instead of treating both as equal when they are distinctively different. At the same time recommending to the ministry that green-crypto might have different tax-implications than black-crypto, as part of a broader national policy related to energy consumption would be good for both Australians and more generally the entire Earth.

Within companies who are doing blockchain applications there are many ways to classify their cybersecurity posture, the two ways I like to use are those which are custodial (using humans for security) & non-custodial (using automated comptrollers) - both have advantages and disadvantages. However the rules & requirements for both are very different, and generally speaking the non-custodial are the technologically 'preferred' but also less common way of operating. A classification system for the types of security controls within the governance structures and an easy-as classification system for the different means is very sensible. For example multi-sig with provable recovery mechanisms should be a mandatory requirement for any human custodial situation to avoid rug-pulls or even 'death by tram' situations that would cause investors to lose out. The other organizations which are non-custodial smart-contracts are going to be subject to all the bad & stupid behaviors that come from having humans handle money.

I do not think a one size or set of rules fits all because that caters to the lowest common denominator. I encourage you to consider this strategy, of having Australia be both a partner, ambassador, and 'investor advocate' (using it's regulatory oversight) for companies that choose to host here and abide by the laws in Australia.

The requirements such as ISO27001 SOC2 etc. are insufficient in that they are reactive cybersecurity postures. The audit requirements are not suitable for small DAO based organizations such as a footy club, or a church. Additionally multisig wallets should be mandatory for any form of custodial governance.

In my mind, the ATO should revisit its position on Crypto-neutrality. Specifically adopting a dual or triple classification, that is revised perhaps once every decade or half-decade.

The first classification “One” is your proposal as written, to support both old ‘legacy’ generation 1 coins such as bitcoin AND emerging fin-tech that does not fit into the second or other future classes. The first class should be inclusive and broad.

The second classification I am proposing is narrow with specific technical qualifications. In order to qualify the organizations must be using automated comptrollers and internal not-human controlled custodial accounts.

The third class I am proposing is an “Australian Stack” which is a simplified, easy-as, set of common sense consumer and regulatory guidance for ‘accepted best practices’. Technologies that enjoy broad support and global consensus to reduce the complexity of choice & risk.
This second class would (for example) include one or more ATO Oracles in the form of solidity smart-contract libraries which *must* be included and provide auditing & ensure operational compliance, provide safety holds on large, white lists of known crypto-addresses for national organizations & black-lists of known bad actors. The second class could offer Australian citizens (or foreigners who pay for the privilege) some level of sovereign debt secured depository guarantee/insurance equivalent to the US FDIC up to a certain amount (which might be as low as $1,000 AU) as a way to encourage crypto-companies to choose Australia as it’s home, and to provide an orderly well regulated safe-harbor “gold standard” that other countries can follow.

For large companies there will probably need to be some sort of national conversation about technology patches, upgrades, refactoring, etc. before any systems could even be considered crypto-ready, in other words widespread adoption of crypto is probably a long way off for average Australian businesses despite many other countries globally celebrating & embracing the advent of smart paperless money. I will provide my suggestions for how I think your consultation paper could be clarified, improved, and perhaps lay a foundation for how to easily accelerate the adoption.

Since definitions which are codified into law must have sufficient word-precision to ensure they are able to distinguish good from bad, right from wrong and this can be incredibly difficult with high-tech jargon which is not always codified.

Right now most Australian blockchain projects are actually centrally controlled but geographically distributed ledgers, and I just want to get that out of the way. I’m not talking about conventional Australian blockchain which is actually “Distributed Ledger”. Australian vocabulary lacks the word precision to differentiate.

So it’s understandable Australia seems to conflate this – I think the Australian tendency to shorten words causes Aussies to miss important details. So I just want to highlight say that centralized models are easier for politicians to understand because historically humanity has operated on centralized governance “Custodial” models which I quite dislike and I hope to convince you by the end of this that Australia would be a better place to live if it encouraged more decentralized technologies because Australia itself is (as I see it) decentralized.

The bad actors will always want to appear like good actors and the national government's responsibility is to provide a mechanism to differentiate the two - this establishes the basis for trust, and allows courts and other means to have a voice in how others on the network treat those actors. This is why network consumable protocols are preferred, those backed with cryptographic controls.

Australia in my limited experience is actually really good at making English things social and simple - it's not at all like my home in America where the people can't tell real from fake news, and so I'm keen on both making my own long term home here but also exporting Australian culture which includes respect, equality, and adherence to the rule of law globally at the speed of light using blockchain technology. I'm going to propose a series of what I hope are simple-as things Australia could do, a plurality of easy-as legislative initiatives that would in my opinion bring an age of blockchain enlightenment (and revenue) to Australia and hopefully export the same to the rest of the planet.

I hope Australia will consider that future foreign companies who are seeking to gain consumer favor may choose Australia if it can strike the right balance of consumer protections through good #governance which is a theme. If you want Australia to be a crypto-favored nation with influence in the future then the time for leadership is now (actually it was a few years ago, but the second best time to start is today).

Remember: Human Custodial governance is fallible. There is a bias inherent in your planning which prefers human custodian because there is a belief the courts have jurisdictional control of the determinism. The mistake of this assumption is the attack surface area, the complexity to describe how to secure a system with human custodians is an order of magnitude more complex. So many possible scenarios surrounding lost, corrupted or compromised wallets easily diminishes any appearance of control, but that is a mirage. Modern human-oriented custodial processes were put in place early in the network design to mimic the software controls as the blockchain networks code matured, however there has been no need for human governance since ~2017 (besides the high barrier of technical complexity, which gets an order of magnitude easier once it is federally codified in protocols that establish trust in formats the blockchain network services can consume).

I will point out during the course of this that Australia having such a highly geographically stratified population across the immense geography is perhaps poised to reap more benefits from decentralization than ANY OTHER nation on planet earth, or it can follow it's current path designed by Politicians who are blockchain neophytes and metaphorically continue to farm with horses & plows rather (human custodians) than utilize the digital currency equivalent of self-driving autonomous tractors (the codified instructions within a smart contract).

NOT all Blockchain crypto-currencies support smart-contracts, although most consumers treat crypto-currencies as tradable commodities like gold, oil and silver this is a 1st generation 'bitcoin' mindset. Trading or treating crypto-coins like commodities has little/no value to society beyond "proof of concept" for the more advanced ideas such as decentralized finance available in subsequent versions.

I would personally suggest Proof of Work is 'fire prone' taxing on the national grid, which is already under significant strain, at least until 2050 or until the national net-zero carbon emission is received, that black-crypto should be subject to a 'black crypto' higher tax rate. This will hopefully tip the favor towards optimization and efficiency, and encourage businesses to adopt more robust protocols that use Proof of Stake (and hopefully voluntary compliance controls from the ATO). Any extra power the country of Australia can generate beyond its own needs, including long term gravity or hydro storage of power should be exported to other countries - not wasted on black crypto "Proof of Waste", and as such people who want to 'invest' in those should be treated just like cigarettes, alcohol, etc. and classified generally as

‘undesirable’ for society from a regulatory perspective.

There are at most conceivably a half dozen second-generation L1 (layer-1) protocols such as Ethereum, and even fewer smart-contract languages (Solidity) that are used. My point is that adding native support for the protocols which are nearly ubiquitous (i.e. you already have a website which offers the HTTP or HTTPS protocol) is a simple extension of your existing service catalog. Deciding when/if you support an L1 network is a big national commitment, and so there should be criteria in terms of ‘when & if’ an L1 network needs to implement AT controls, but again - if you use ‘finger’ controls then I'll dare say it’s 100% ubiquitous & easy to implement the one finger service, for potentially dozens or even hundreds (or maybe even tens of thousands) of distinct forms of technical control’s on/in the blockchain network and more broadly within organizational structure & governance.

Crypto-currencies are digital money, and smart contracts are the equivalent of being able to write instructions on an envelope containing money describing who, how and when the money inside the envelope can be spent. The network will enforce the governance provided it was incorporated before the project is live, suddenly the indicator (or absence) of governance controls is easily auditable in a programmatic fashion (like a virus scanner, except it’s a smart contract governance linter).

One aspect the Australian government must do is identify which blockchains it will “support”, and the tax aspects of conducting business using crypto-currency. This is an area which is probably beyond the scope of this paper - however suffice to say many aspects of the national operation could be efficiently streamlined by rapid adoption of smart-contracts over the next decade.

By the ATO stablishing its own central registry “Source of Truth” of national ABN’s, (just like chinese ICP licenses), mapping those identities to wallet addresses, requiring certain types of transactions such as real-estate to traverse through well known ‘registered’ entities. This is important because I want a way to know that a future digital deed NFT for a piece of property is valid, so the ATO is one signal of trust that the organization I’m dealing with can obtain an ATO stamp (which I can very mathematically verfiy using the key either I or my program downloaded from the ATO finger server). This very simple approach gives you nearly infinite expandability potentially even on a case by case “voluntary & cooperative” basis.

Rather than requiring each company to perform its own KYC the AUS should allow individuals or companies to register on the vetted list, and denote the type of actor such as individual, national corporation, or foreign entity. The ATO can do a lot to help the Australian crypto community make stuff easier too is my point - so this is another reason I’m not advocating for the industry-self regulating. I am not advocating for an in-voluntary (compelled participation) route at this stage - but I am encouraging adding regulatory safeguards today using technical protocols.

There are community processes for developing these, in terms of developing software and no more so than using the GIT protocol. One nice aspect of GIT (a version control system for software development) is perhaps the most appropriate tool for developing some of the systems. Having major cloud vendors such as Microsoft, Amazon, Google all use the protocol internally and allow those companies to host an official mirror copy of the archive in their clouds. (Microsoft already gives away free hosting of this on the service known as github, so they would definitely say - no problem). Perhaps the most famous and successful Australian technology startup “Atlassian” is built on the top of the GIT protocol for all their tools. Again, any laws, rules, etc. related to crypto should refer to a git repository & version # or tag/naming convention.

Further the Australian government should plan to publish a list of known or suspected bad actors for its

citizens to use to avoid scams and ensure sanctions. The simplest form of 'black-listing' (or in more 'woke' syntax, ban-list, or "red-flag") is a text file with known bad actor wallets addresses hosted in a text file. Allow cyber-vigilantes such as myself to legally attack & recover funds from those wallets, in exchange for a portion of the proceeds 'reward'. Having the 'symbolic authority' to add new entries to the "dodgy-erc20-wallets.json" file, technically might "mean something" as a court remedy, and gain, that same file can be managed from git and distributed by finger (or HTTP, or SMTP/email or whatever automated services you decide to offer). This approach provides clear lineage of funds, it provides a way to say that a transaction when it occurred was/is being performed by what is believed to be a legitimate (or illegitimate) actor.

Smart contract behaviors can be tested for compliance using linting, part of this process will deploy or copy the smart contract onto a fake 'clone' of the network and 'exercise' the governance code through a process known as test driven development or commonly abbreviated to TDD. Using TDD code is run in simulations to make sure it deterministically performs as expected, i.e. each function with a short-circuit does actually short-circuit as requested. Short circuit is just one of potentially dozens or hundreds of behaviors that might need to be tested - but since these are done programmatically, often in parallel they only take a few seconds to run - amazing efficiency!

Smart-contracts are an important part of the decentralized finance movement which could disruptively benefit a number of both marginalized groups & important future industries covering all aspects of Australian society from banking, physical and digital property ownership, and sports wagering. Australia Treasury should PROBABLY someday have/offer DAO templates, approved templates for 'easy-as' governance, that can be forked and thus has a governance template allowing a person to participate in potentially multiple DAOs as officers, directors, or any other contributing role the DAO allows. Rather than allowing each club to make their own, by giving them a common template will increase uniformity and also allow developers to move between/across/within AU organizations faster & with less difficulty.

Smart contracts are programs which are executed by the network of computers running the blockchain. DAO's are an organizational code, they have voting and other forms of organizational governance. Conceptually this is equivalent to indelible digital bylaws written in executable code, it's actually quite attractive from a regulatory standpoint since by nature any deviation from those encoded rules.

Indelibility is important, because it means the instructions cannot be circumvented by any person or court, the only way for a smart contract to be circumvented is by a majority of the computers on the network operating the blockchain across the entire globe to coordinate all update to a new version of the blockchain software that overwrites something the entire network "wants to reverse", so it is in the best interest of future nations to ensure they have a sufficient number of computers operate the network that their economies depend on and coordinate peacefully with their neighbors. Adding somebody to the "dodgy-wallet-erc20.json" (as an example) can also be consumed by coin exchanges etc. as a way to vet or potentially reappropriate stolen funds - what good is stealing money if it suddenly becomes invalid and unspendable "shunned", forcing criminals post rug-pull to use high-risk crypto-tumblers (which themselves could be ethical hacker-run recovery honey-pots for crypto-scam bounty-hunter remuneration).

Unlike conventional software which on a computer can be corrupted or have bugs causing crashes, smart-contracts are run by a network of computers and should be designed in a way where they are both observable & recoverable.

Final summary:

- Use word precision, when making up new words - start with "proof of waste"
    - We as a society do not need to embrace first generation " PoW " Proof of Waste.

    - It would be better to basically try and do whatever you can to treat bitcoin ‘black crypto’ like you do tobacco. By discouraging use of black-crypto you may help the national goals toward policy climate change and not burning people & animals alive from electric grid fires.
    - A more wasteful energy footprint is less favorable (electric grid stress causes fires).
- Use existing standards rather than inventing new ambiguous terms.
    - When adopting technical standards embrace protocols which can perform governance, that have the features & functionality which are prone toward solving real Australian problems.
    - Ethereum as an L1 would be a great place to start since it has the ability to implement all the features I described (and at least a hundred more I didn’t).
    - Anything can can be done on Ethereum (or the Solidity programming) can be done with 1/10th the effort on every other blockchain because Ethereum is a ‘reference’ L1 protocol that every chain universally uses. (I.e. ERC-20 for a wallet is Ethereum request for comment, but all L2 Ethereum chains, and even non Ethereum L1 chains such as Solana, virtually all L1 chains use ERC-20, it’s ubiquitous). Solidity also compiles to both Solana and Ethereum (and many others), so that is a good choice - to use polyglot technologies for ubiquitous support.
- Provide signing & recovery authority via finger or equivalent protocol
    - I’m not going to explain what this means (again), exactly, because time, but generally if you want to know more - and there is A LOT of ways to do this here, it would almost require it’s own paper(s) on the ways you could do this.
    - What I will say on the topic is simple: put in Australian smart-contract function “wrappers” that can only be called from a smart contract, if you want to host that on a distributed ledger which you call a blockchain but is actually a centrally controlled geographically distributed ledger that’s fine, just word precision.
- AICD, GIOA & Idiomatic Syntax / Awareness & Technical vocabulary in the board room
    - The reality is crypto-currencies are going to need and require more technical board members. Embrace this by unifying the regulatory and industry vernacular. Using the git tool the ATO can easily publish your changes or new features to the specifications in a versioned format using industry standard tools. (Git as tool is more than 20 years old, but still not widely adopted in Australia - but it is by far the most common tool globally)
    - Discuss the non-custodial governance, which should be done in coordination with the AICD & GIOA - that would be an “all in”, then you develop and Aussie contract syntax, in idiomatic style, that says how things should happen.
      This idea of transpilation is a concept borrowed from compilers, and it basically means a document that can be translated from Australian into smart-contract ese, approved “words” and “terms” with precise definitions that can be executed as code, but also written in a programmatically executable way. The pioneer of this idiomatic syntax style, I can’t take credit for it – the idea was given to me by a guy named Donald Knuth who is sort of a legendary smart person in my field of software & computer science. He’s a big fan of these compositional approaches.