Great Australian DAOs

A Proposal for Recognising Decentralised Public Networks and Their Digital Assets Under Australian Law

Scott Robert Chamberlain
ENTREPRENEURIAL FELLOW, ANU COLLEGE OF LAW

Great Australian DAOs

A Proposal for Recognising Decentralised Public Networks and their Digital Assets Under Australian Law

Foreword

In its hearing on 27 August the Senate Select Committee on Australia as a Technology and Financial Centre challenged the panel members to develop proposals to regulate Decentralised Autonomous Organisations (DAOs) without relying on a new corporate form. This proposal answers that challenge.

Sources of Federal Government Power

Regulating DAOs means creating special rights, liabilities, and immunities for certain relationships conducted via blockchains and smart contracts. There are two potential sources for the Commonwealth's constitutional power to regulate such relationships, even if the Committee's injunction against new corporate forms means the more traditional "corporations power" (Article 51(xx)) must be excluded.

Those two sources are:

> **Article 51(v): "postal, telegraphic, telephonic and like services"**
>
> This power is the basis of commonwealth laws regulating the internet and cybersecurity. It includes using the internet and telecommunications infrastructure and almost certainly includes using those things to form, manage, and participate in distributed cryptographic systems like blockchains and smart contracts.
>
> **Article 52: "the territories power"**
>
> The federal government has plenary power over its seat of government (the ACT) and its Territories. Article 52 would be a fall-back option that would allow some form of registration and regulation of DAOs in the ACT where at least one node (Anchor node) is based in the ACT. It is an unwieldy option.

This proposal assumes a law founded on Article 51(v).

From Incorporated DAO to Unincorporated Relationships

The Wyoming concept of a DAO is of a corporate entity that has code as its constitution, does not have a board, but which gives its users limited liability. Translating these characteristics into a non-corporate entity means creating a new type of relationship and defining the rights, liabilities, and privileges between people in that relationship and between those people and third parties.

Partnerships are an example of a relationship regulated in this way. A partnership is not a separate legal entity. While assets and profits are pooled and shared, each partner is separately liable for their own tax. Partnerships are recognised by common law and are regulated by State legislation. But this relationship is not suited to DAOs because each partner is jointly and severally liable to third parties for the acts of any user of the partnership.

An alternative relationship is the unincorporated joint venture. Properly structured, these are not partnerships. Parties share the outputs (not profits) from their collaboration, bear their own costs, and tend to retain ownership of their inputs. While the joint venture tends to be co-ordinated through a management committee, the parties are severally liable to third parties for their own actions, pay their own tax, and retain their own insurance.

Introducing the "decentralised public network"

This proposal adopts the unincorporated joint venture model. It creates a special type of unincorporated joint venture – called a "decentralised public network". Under this model, the code is the network's rules, and the users have no liability to each other and limited liability to third parties for their participation in the decentralised public network, excluding crime and fraud. The overarching aim is to reinforce user's reliance on their network's code, and not the law.

Structure of this Proposal

This proposal assumes an Act ("the Act"), founded on Article 51(v) of the Constitution, that defines the rights, liabilities, and immunities of persons who use decentralised public networks and decentralised smart contracts to create, manage, and participate in such networks. It provides the key proposed sections that might appear in such an Act. After each section, commentary is offered to highlight the reasoning behind each proposed section.

The Breadth of This Proposal

Wyoming's incorporated DAO provisions do not exist in isolation. They were part of, and relied upon, a comprehensive reworking of Wyoming law to make a home for blockchains and digital assets in their jurisdiction. For this reason, the proposal outlined below does not simply deal with a non-corporate form of DAO. It includes many adjustments necessary to make a home for digital asset projects in Australia. Those adjustments provide the "legal infrastructure" necessary for the new concept of decentralised public networks to work in Australia.

Next Steps

I'd like to thank my friend and colleague, Richard Holland, for his invaluable time and expertise in helping refine this proposal, particularly the definitions.

I am happy to discuss any further questions or issues arising from this proposal.

Scott Chamberlain
16 September 2021

Proposed Laws

1. Decentralised Public Networks

Definitions

1.1 In this Act:

(a) **Centralised network** means a network that has ceased to be a decentralised public network because of section 1.6.

(b) **Decentralised public network** means a publicly accessible network of multiple independently owned computers that exhibits all the following attributes:

(i) Each computer runs compatible code that uses a byzantine fault tolerant consensus protocol to agree on and maintain a canonical shared state across multiple computers.

(ii) The code each computer runs to be part of the network is open-source code.

(iii) The network's canonical shared state is public.

(iv) The network uses a public key pair cryptography scheme to authenticate messages submitted on the network.

(v) Anyone can create a key-pair to become a user of the network, even if not all users have the same use rights.

(c) **Key pair** means the mathematically or algorithmically paired public key and its corresponding private key (or combination of private keys through a multi-signature arrangement), or substantially similar analogue, such that a message signed with the private key can be authenticated using the public key.

(d) **Multi-signature arrangement** means a system of access control in which two (2) or more private keys are required to sign and submit a message, or any substantially similar analogue, to a decentralised public network.

(e) **Open-source code** means, in respect of a network, software source code that is publicly available to use and modify without charge for purposes associated with that network, even if it is not publicly available free of charge for other uses or purposes.

(f) **Private key** means a unique element of cryptographic data, or any substantially similar analogue, which is:

(i) Held by a person.

(ii) Mathematically paired (alone or in combination with other private keys through a multi-signature arrangement) with a public key.

(iii) Associated with an algorithm that is necessary to cryptographically sign and submit messages on a decentralised public network.

(g) **Public address** means a payment endpoint for digital assets on the network typically, but not always, derived from or associated with a user's public key.

(h) **Public key** means the unique, publicly available element of cryptographic data, or substantially similar analogue, of a key pair.

The challenge of this section is to define the network in such a way to capture all the ways people might use decentralised public networks to govern their relationship, but to exclude all the centralised, closed options.

The definition of decentralised public network is designed to cover those blockchain projects that are "genuinely" decentralised. There will be many blockchain projects that do not, or cannot, fit this definition, and that is its whole point. The protections from liability that this Act is designed to achieve should only apply to those networks that anyone can join, everyone can police, and nobody owns.

It covers the whole of the network and not just DAOs defined by smart contracts running on a network. This is because such blockchain projects are just big DAOs, especially if the users have some form of governance role.

The requirement that the code be open source is crucial. It means the network is genuinely choosing to rely on the code and can police its operation. The distinction between open-source and closed sourced code becomes important in defining the limits of any immunities granted to users of decentralised public networks.

Creating a Decentralised Public Network

1.2 Any person may create, manage, support, maintain, join, or use a decentralised public network.

1.3 No person contravenes any law by providing any good or service they are otherwise lawfully able to provide to help create, manage, support, maintain, or use a decentralised public network.

Nature of Decentralised Public Networks

1.4 A decentralised public network:

(a) Is not a separate legal entity.

(b) Is not a venture, partnership, joint-venture, or common enterprise.

(c) Cannot sue or be sued.

(d) Cannot hold any property other than the digital assets existing on its network.

1.5 No person may:

(a) Register, or be required to register, a decentralised public network or public smart contract for any form of tax.

(b) File or be required to file, any type of tax return for or on behalf of a decentralised public network or public smart contract.

These sections confirm a decentralised public network is not a legal entity and removes it from the definition of many things our law treat as legal entitles even though they are not (like "ventures" and "enterprises"). This is fundamental to the requirement that we not create a new corporate form.

The provisions relating to tax clarify these communities are not tax entities. As obligations embedded in the real world, they are neither analogous to corporations nor bureaucrats. Rather they are like the poles-and-strips that define orderly queues at an airport. It makes no sense to tax these entities any more than tax to ribbons that define a queue.

Loss of Decentralised Public Network Status

1.6 A network that is otherwise a decentralised public network ceases to be a decentralised public network if for more than consecutive 24 months:

(a) Less than 20 computers comprise the decentralised public network.

(b) Less than 20 independent persons operate the computers that comprise the decentralised public network.

(c) Its developers and promoters (alone or through a multi-signature arrangement) retain preferential rights to unilaterally edit or disable the code the network runs, including through mechanisms such as a kill switch, a master set of private keys, or manufactured dominance of governance rights.

1.7 A network to which 1.6 applies is a centralised network from that time until the conditions specified in section 1.6 no longer apply to the network.

These sections are about ensuring a decentralised public network grow within a reasonable time to become "truly decentralised". A network with insufficient independent actors or independent control ceases to be a decentralised public network.

In objectively defining truly decentralised, the provisions use 20 computers as an objective threshold number. This number is a common threshold identifying organisations that are small and private. If a blockchain has less than 20 validators or less than 20 genuine members it is probably not public and decentralised. It could/should use existing corporate forms, if necessary.

Even decentralised public networks will start off small. They won't ever grow to more than 20 computers if they are not given immunities while they are small. We have recommended a 24-month window for any network to demonstrate that it can grow to, and sustain, the 20-computer/20--independent operator threshold.

Nature of Centralised Networks

1.8 Unless the operators otherwise agree, from the time it ceases to be a decentralised public network, a centralised network is:

(a) A common law partnership between each operator of a computer on the network if established for profit or gain.

(b) An unincorporated association of which each operator is a member if established not for profit.

Finally, the section clarifies the nature of those centralised networks that fall outside the definition of a decentralised public network.

The default us a common law partnership or unincorporated association. Centralised networks that want a different classification probably have the means to adopt a different corporate form because of their centralisation.

2. Smart Contracts

Definitions

2.1 In this Act:

(a) **Smart contract** means a collection of code and data deployed to multiple (but not necessarily all) computers on a decentralised public network that users interact with via messages cryptographically signed with their private key.

(b) **Network smart contract** means a smart contract where all the following is true:

(i) Any user of the network can interact with it.

(ii) All its code is open-source code.

(iii) Its code cannot be changed or disabled, except through a governance process open to all users by virtue of being users of the network.

(c) **Community smart contract** means a smart contract where all the following is true:

(i) All its code is open-source code.

(ii) Its code can be changed or disabled by a sub-set of the network's users, such as those that interacted with the contract or who own governance tokens or some other right not available to other users by virtue of being a user of the network.

(d) **Developer smart contract** means any smart contract that is not a network or community smart contract, and includes a smart contract where any of the following is true:

(i) Any part of the code is closed source.

(ii) Its developers and promoters (alone or through a multi-signature arrangement) retain preferential rights to unilaterally edit or disable the contract, including through mechanisms such as a kill switch, a master set of private keys, or manufactured dominance of governance rights.

This section reduces the vast universe of possible smart contracts into three categories based upon who can alter or disable their code. Network contracts are controlled by the entire network. Community smart contracts are controlled by a sub-set of users on a network. Developer smart contracts are controlled by the individual or small team that developed or deployed the contract.

Nature of Smart Contracts

2.2 A network smart contract is part of the network for all purposes of this Act.

2.3 A community smart contract is a user of the network for the purposes of this Act, but one that lacks legal personality and so has no legal capacity to contract or to engage in personal conduct.

2.4 A developer smart contract is an agent of the developer such that anything done by the developer smart contract is deemed done by the developer as a user of the network.

This suite of definitions gives an appropriate legal characterisation for each potential type of smart contract.

Network smart contracts are indistinguishable from the network itself. Their code is public and can't be changed unless the network changes. They are treated as part of the network.

*Community smart contracts are a special type of user of the network, one that can control digital assets but doesn't have separate legal personality. They *are* their code and users interact with that code at their own risk because it is public.*

Developer smart contracts are not public or can be changed unilaterally by a very limited set of privileged users. These smart contracts are legal agents of the people who deployed them or control them. Anything done by a developer smart contract is deemed done by that developer.

3. Users

Definitions

3.1 In this Act:

(a) **Network conduct** means:

(i) Creating or destroying a key pair, or any similar analogue for becoming or ceasing to be a user of a network.

(ii) Operating a computer on the network.

(iii) Using or refraining from using a private key to cryptographically sign and submit a message to the network, or any similar analogue.

(iv) Deploying or using a network smart contract or community smart contract on the network.

(b) **Personal conduct** means doing anything that is not network conduct or refraining from doing anything, that if done, would not be network conduct.

The challenge of this section is to mimic the limited liability shareholders receive despite there being no corporate entity. The start of this process is to draw a distinction between network and personal conduct.

Network conduct is effectively things users can do "on-chain". Personal conduct is things users do in the real world. This mimics the distinction between things shareholders do by virtue of being shareholders (for which their liability is limited) versus everything else they can do.

Note that deploying or using a developer smart contract is personal conduct. This is because such contracts are private. Third parties should not be treated as having agreed to use those contracts at their own risk.

Users

3.2 In this Act, a user of a decentralised public network is:

(a) Any person who holds a private key used to interact with that network (alone or as part of a multi-signature arrangement)

(b) Any person who controls a computer or device that holds a private key used to interact with that network (alone or as part of a multi-signature arrangement).

The section defines a user of a network as being a person who holds a private key or the person who controls any device that holds such a key. This is necessary because often the use of the private key is automated inside a software program, not physically entered via human action.

Assumed Risks

3.3 Each user of a decentralised public network is deemed to have expressly consented to all the following the moment they hold a private key:

(a) To assume all risks associated with using the network to mediate their dealings with other users of the network.

(b) To any public disclosure of their personal data arising from anyone's use of the network.

The section confirms users of a decentralised public network do so at their own risk. The rationale is that since the network is open and public, the users are choosing to trust the code and little else. Because it is essential the network be public, users are deemed to have consented to the network's use and publication of their personal information.

Secrecy of Private Keys

3.4 No person may ever compel any person to reveal any private key they hold.

The section adopts the position taken in Wyoming. It confirms a user cannot be compelled to reveal their private key. This is necessary because the relationship between digital assets and private keys means whoever knows the key virtually owns the asset.

Note, however, that other sections provide that a user can be compelled to use their private key to execute transactions to the extent such transactions are permitted by the network's code.

Relationship Between Users

3.5 Except as otherwise provided in this Act and unless a user otherwise contracts with another:

(a) No legal relationship of any kind exists between the users of a decentralised public network, including as agent, partner, trustee, employee, co-venturer, or contractor.

(b) No user is answerable to any other user for their network conduct.

(c) No user has any right or authority to bind any other user.

(d) No user is ever liable to any other user for the performance, function, or reliability of the network.

3.6 Each user of a decentralised public network forgives and forever indemnifies each other user from and against any claim the user has or may have against any other user for any loss or damage the user has or may suffer have arising from their network conduct.

This section confirms that users have no legal relationship or liability to each other by virtue of being users of the same network.

This is necessary because users are assumed to have agreed to relate solely through the public code on their open network. If users were in a legal relationship the network would become inherently centralised because users who believe the network has treated them unfairly would always be able to seek legal redress against somebody – or everybody. This section ensures users must rely on the code unless they specifically take steps to agree something else.

Again, it should be noted this only applies to users of decentralised public networks. No immunity applies to things done through closed-source code. If nobody has the can view, audit, and police the code, nobody can be presumed to have agreed to rely on the code and not the law in mediating their relationship.

Relationship to Non-Users

3.7 A user of a decentralised public network is not liable in civil law or equity to any non-user of the network for any kind of loss or damage arising in any way from:

(a) Their network conduct.

(b) Any other user's network conduct.

(c) Any other user's personal conduct.

But always remains liable to non-users for loss or damage arising from their personal conduct.

This section gives users no liability to third parties for what they achieve on-chain through open-source code, makes them liable individually for their own conduct off-chain, and never gives them any immunity for conduct that constitutes a crime or fraud. This formulation is seen as a reasonable proxy for the limited liability users would receive if the network was treated like an incorporated entity as per the Wyoming model.

Assumed Contractual Obligations

3.8 A user who contracts with any person to engage or refrain from engaging in any specific network conduct or personal conduct ('the promised conduct') must engage, or refrain from engaging, in the promised conduct.

3.9 A user contractually bound to any person to engage in any network conduct (the promised network conduct):

(a) Warrants they will take, or refrain from taking, the promised network conduct.

(b) Neither warrants nor assumes any liability for how the network will perform, if at all, because of them engaging in the promised network conduct.

This section again mimics the position of shareholder's in companies. They are liable for contracts they make in respect of their shares. So, here, it is proposed that users should always be liable for contracts they make in respect of the network access rights bestowed by their private keys.

Full Liability for Crime and Fraud

3.10 Every user is always liable to anyone who suffers any loss or damage arising from their illegal or fraudulent conduct.

Nobody gets any immunity to commit crimes or engage in fraud.

4. Digital Assets

Definitions

4.1 In this Act:

(a) **Digital asset** means a representation of economic, proprietary, or access rights stored in the canonical shared state of a decentralised public network which is self-contained, uniquely identifiable, and has a value or use.

(b) **Network token** means a digital asset that is an unbacked medium of exchange or unit of account on a network with no identifiable counterparty other than the network itself.

(c) **E-Money token** means a digital asset that is not a network token and satisfies at least one of the following:

(i) It represents a deposit of an equivalent value of sovereign fiat currency.

(ii) It represents a promise or understanding to redeem the token for a fixed value of a sovereign fiat currency, or goods or services of equivalent value.

(d) **Security token** means a digital asset that:

(i) Is not an E-money token.

(ii) Embodies rights to financial returns from, or interests in, investment vehicles of the kind emblematic of securities.

(e) **Ownership token** means a digital asset that:

(i) Is not a security token:

(ii) Embodies rights or claims to tangible or intangible property.

(f) **Utility token** means a digital asset that is not any other kind of digital asset, typically those embodying on use or access rights to networks, services, or memberships.

The sections defines digital assets then arranges them into four different types of tokens for the purposes of regulatory compliance. These categories mirror those adopted in the UK, except for a new category for "ownership tokens", being digital assets that embody ownership rights to tangible or intangible property.

Creation of Digital Assets

4.2 A digital asset:

(a) Exists the moment it becomes controlled by a user.

(b) Does not exist until it first becomes controlled by a user.

(c) Ceases to exist the moment it ceases to be controlled by any user.

The section clarifies that digital assets only exist while controlled by a user. So once an asset becomes controlled only by the network it ceases it to exist. This is necessary because the network has no legal personality. The assets only exist in relationship to users of the network, not in relation to the network itself.

Nature of Digital Assets

4.3 On creation, a digital asset is a chose in possession:

(a) Possessed by the user that controls it.

(b) Capable of assignment at will.

(c) Capable of being the subject of a security interest or trust.

(d) Even if it was intended on creation to embody rights or claims otherwise indicative of a chose in action.

The section defines digital assets as personal property capable of assignment at will and being the subject of a security interest or trust. This resolves a major ambiguity with the nature of digital assets. This only applies to assets on decentralised public networks. Assets on other types of networks may not be property.

The section defines digital assets as choses in possession, even if they embody rights that would otherwise be choses in action. This is necessary because choses in action often have legal restrictions on assignment. But these assets can trade at will on decentralised public networks. If a counterparty wants to restrict who can own or trade an asset that embodies rights against them, they need to use the network's rules, not legal authority to enforce such restrictions.

Regulation of Digital Asset Classes

4.4 Exchange tokens and e-money tokens are always a **digital currency** within the meaning of the *A New Tax System (Goods and Services Tax) Act 1999* and the *A New Tax System (Goods and Services Tax) Regulations 1999*.

4.5 E-money tokens are subject to the same laws and regulations as equivalent money, payments, and deposits.

4.6 The counterparty of any e-money token is a *holder of stored value* for the purposes of the *Payment Systems (Regulation) Act 1988,* unless the nature of the relevant token is such that some other characterisation or exemption is relevant (for example, if the token is not assignable and is simply credit redeemable for the merchant's goods and services.)

4.7 A security token is a *security* for the purposes of the *Corporations Act 2001* of the type most analogous to the type of rights or claims against the identifiable counterparty they were intended to represent upon creation.

4.8 Ownership tokens are regulated the same way as the underlying tangible or intangible property rights they represent.

4.9 A utility token takes on whatever character best describes the nature of the rights the token represents or was intended to represent on creation.

This section gives each token type its natural regulatory "home" in Australian law, again modelled on the approach in the UK.

Exchange tokens are digital assets native to their blockchain. These assets have no counterparty. They exist because the network exists, and they do whatever it is the network lets them do. These tokens are treated as digital currency for the purposes of GST.

E-money tokens are digital assets that represent money. It would include fiat-backed stable coins. These are regulated in the same way as equivalent forms of money, deposits, and IOUs.

Security tokens are digital assets that have rights or claims like traditional securities. They are regulated like the securities they mimic.

Every other type of digital asset is a utility token. This category is necessary because the definition of digital assets includes a wide range of access or use rights – data that identifies things you can or cannot do within the network. Provided these things are not any other type of token, they take whatever character best fits the rights they embody.

5. Owners of Digital Assets

Definitions

5.1 In this Act:

(a) **Digital asset reward** means a digital asset that comes into a user's control because of:

(i) Their control of other digital assets.

(ii) Their usership of the network.

(iii) Their network conduct.

(iv) A change to the decentralised public network's rules.

(v) A fork of any part of the decentralised public network's rules.

(b) **Digital asset exchange service** means:

(i) any person in the business of exchanging or facilitating the exchange of digital assets for digital assets or of digital assets and currency to, from, or between customers.

(ii) any designated digital currency exchange service within the meaning of section 6 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*.

But does not include customers of such a service who carry on a business of trading digital assets with other customers or the operator of the service.

Control of Digital Assets

5.2 A user controls a digital asset if the user holds a private key that can (alone or as part of a multi-signature arrangement, but independent of any other user) cryptographically sign and submit a message to a decentralised public network that:

(a) Exercises any type of access right or function because the network exclusively associates that digital asset with the user.

(b) Removes the digital asset from its exclusive association with the user.

(c) Moves or returns that digital asset to its exclusive association with the user.

or any substantially similar analogue for the user having exclusive, independent control of the digital asset or of the access rights associated with control of the digital asset.

*There is a necessary distinction between ownership and control of digital assets (one reason they are defined by default as choses in possession by earlier sections). This section confirms that *control* is about the independent ability to exercise network functions related to the digital asset because the network associates the digital asset with the user.*

Note that a user who "deposits" assets into a community smart contract they can later redeem is deemed to retain control of those assets (making the smart contract a custodian of the assets in later sections)

Ownership of Digital Assets

5.3 A person who controls a digital asset owns that asset unless they acquired control of the digital asset in bad faith or with actual or constructive knowledge of another person's prior claims to the digital asset.

5.4 A person always has actual or constructive knowledge of another person's prior claims to a digital asset if they hold the private key that controls the digital asset:

(a) Through illicit or dishonest means.

(b) On the express or implicit condition or understanding that it would only be used with the consent of the digital asset's legal owner.

(c) As part of a multi-signature arrangement established by the digital asset's legal owner.

5.5 For clarity, a person need not be a user of the network to be the lawful owner of a digital asset.

5.6 The customers of a digital currency exchange service are always the legal owners of the digital assets the operator holds on their behalf.

This section begins with the general rule that a person possesses a digital asset if they know the private keys that control the asset, but they have good title to a digital asset only if they acquired it in good faith without actual or constructive notice of a third party's prior claims. This provides greater certainty than the common law under which good title can be acquired only from those who have it.

This gives digital assets negotiability. It is important that other users be able to assume that, barring bad faith or prior knowledge, they acquire good title to the asset from the person who possesses it. Otherwise, the common law rule that you can only give what you have would lead to endless (and probably fruitless) litigation between users.

Airdrops, Forks and Staking Rewards

5.7 A user of a decentralised public network is deemed to have acquired a digital asset reward at the earliest of the following times:

(a) If:

(i) they were required to do anything within the rules of the decentralised public network for them to control the digital asset; and

(ii) they did those things in expectation or understanding they would receive the digital asset reward,

then the moment the digital asset came into their control.

(b) In any other case – the first moment they initiate any valid transaction within the rules of the decentralised public network in respect of any of the digital asset rewards.

There are many ways networks and smart contracts give users control of digital assets without the user necessarily doing anything to acquire that control. These things are generally a type of reward – a new asset that arises from a network or a smart contract as an airdrop, staking reward, or the consequence of a network fork.

*This section clarifies when a user is deemed to control and own these assets. It is important because of the tax consequences. Users need to be able to *not claim* ownership and control to avoid holding assets they don't desire or attracting unwanted tax liabilities.*

Digital Currency Exchanges Warrant Good Title

5.8 Any person who operates a digital currency exchange service warrants to all users of its service that every person who purchases digital assets using their service acquires good title to their digital assets.

5.9 The operator of a digital currency exchange service must compensate any person whose digital assets are sold via their digital currency exchange service exchange by another person despite their competing prior claim to ownership if the digital asset exchange has actual or constructive knowledge of their prior claims.

5.10 The operator of a digital asset exchange service is deemed to have actual or prior knowledge that a digital asset is the subject of prior claims if:

(a) Either the alleged lawful owner of the digital assets or a reputable blockchain explorer and analysis business advises the operator in writing that the digital assets arriving from one or more public addresses are allegedly tainted by prior claims.

(b) It is unreasonable for the operator to conclude the claim of prior interest is without merit.

5.11 If the operator of a digital asset exchange service receives a digital asset that it reasonably believes is subject to a prior claim, the operator:

(a) May do one of the following:

(i) refuse to accept the digital asset.

(ii) Accept the digital asset but hold it separately on trust until the competing claims are resolved, or otherwise directed by law.

(iii) Transfer the digital asset within 21 days to the party it reasonably believes is the rightful legal owner.

(b) Must advise both parties of the identity and contact details of the other.

5.12 An operator of a digital asset exchange service is not liable for any loss or claim on behalf of any person arising from its exercise of its rights and obligations under section 5.11.

To better protect consumers, there are special rules dealing with good title and digital asset exchanges. Digital asset exchanges are the main touch point between code-governed communities and the outside world. They are the main point through which ill-gotten assets are liquidated into other assets or fiat currency.

First, the section imposes obligations on exchanges to warrant good title to all who purchase from their platforms. Secondly, it must compensate any person whose stolen assets were sold through the exchange if the exchange had prior knowledge. Further, it deems the exchange to have knowledge advised by a reputable block explorer/forensic business that the assets come from a tainted or blacklisted address.

Finally, the section gives the exchanges certain powers to deal with assets they believe may be tainted by prior claims and gives the exchange immunity from legal suits for exercising those powers.

Security Interests in Digital Assets

5.13 Subject to this Act, no user of a decentralised public network has any obligation in law or equity to any person to deal in any way with any digital assets they own and control except as permitted by the network and any smart contract.

5.14 Despite section 5.13, a digital asset a user owns may, because of the user's personal conduct, be the subject of a security interest.

5.15 The user who owns and controls a digital asset subject to a security interest:

(a) Must, so far as is possible, given the rules of the decentralised public network:

(i) Use their private keys to give effect to the security interest.

(ii) Refrain from using their private keys contrary to the security interest.

(b) Cannot, unless otherwise agreed, be held liable for any breach of the security interest except to the extent that breach arises from their non-compliance with section 5.15(a) (for example, if the asset is destroyed because the network fails, or its users vote to implement code changes).

This section begins with a blanket statement that users are not obligated to deal with assets in a way that is incompatible with the network's rules. This aims to prevent things like class actions against all users to enforce rights inconsistent with the open-source code.

However, since digital assets are property, users can, by their own off-chain actions (like verbal promises or formal contracts) create a range of interests in favour of third parties over their assets.

A user who has created such interests must use their private keys in a manner consistent with those interests, so far as is possible. But the user is not liable for other losses provided they comply with this requirement: rights of third parties are non-recourse beyond what the rules of the code can deliver through use of the user's private key.

Disposal of Digital Assets

5.16 A user no longer owns a digital asset the moment all the following are true:

(a) They cease to control of the asset within the meaning of section 5.2.

(b) They either have no legal rights, or have abandoned any legal rights they might have, to compel another user (for example, as a custodian) to sign and submit a message with that other user's private key that would constitute control under section 5.2

This section confirms when a person ceases to own an asset. Since ownership is about legal rights, it is not necessary for a person to be a user of a network to be the owner of an asset. Also, it is possible for a user to cease being the owner of a digital asset even though they remain the person in control of it.

6. Custodians of Digital Assets

Definitions

6.1 In this Act:

(a) **Custodian of a digital asset** means a person who controls a digital asset they do not exclusively own, and always includes:

(i) The operator of a digital currency exchange service in respect of the digital assets its customers have left in the operator's control.

(ii) A community smart contract in respect of the digital assets it controls because of users' interactions with the contract.

(iii) The developer of a developer smart contract in respect of the digital assets they control because of users' interactions with the contract.

The definition of custodian means these sections are about the role of people who control an asset but do not legally own it. Certain types of smart contract are subject to the definition because of their potential to control assets other users own.

Community Smart Contracts as Custodian

6.2 As a custodian, a community smart contract holds all digital assets its controls subject only to its code and the performance of the network on which it runs.

6.3 No user of a network has any claim against anybody in respect of any loss or damage suffered because of a community smart contract's custody or non-custody of their digital asset.

*This section deals with the special problem of community smart contracts as custodian. These contracts are not legal entities. They *are* their code. So, this section confirms these contracts have no legal obligations about how they deal with assets – they hold them subject only to their code – and users who divest control of their assets to such contracts do so completely assuming the risks involved. This is justified on the basis that these contracts are public and immutable except by the community that uses them.*

Custodians Other Than Community Smart Contracts

6.4 Unless otherwise agreed in writing, the custodian of a digital asset (other than a community smart contract) always holds that digital asset on trust for the benefit of the legal owner of the digital asset.

6.5 A custodian of a digital asset (other than a community smart contract) must not, without the express consent or direction of the legal owner of the underlying digital assets:

(a) Deal with the digital asset.

(b) Create a trust or security interest of any kind over the digital asset for the benefit of any third party.

(c) Apply the digital asset for its working capital of to satisfy its creditors.

(d) Lend the digital asset.

(e) Fail to pass through to the legal owner all digital asset rewards that accrue to the custodian by virtue of its control of the relevant digital assets.

This section confirms that all legal entities who have control without ownership hold the assets on trust. That includes developers controlling developer smart contracts and users who acquire control without acquiring good title. The requirement that custodians hold these assets on trust is necessary to prevent the assets from being used to meet the custodians own creditors. Wyoming used a bailor/bailee arrangement. This proposal uses trust relationship instead because of the risk under Australian law that digital assets held by a custodian but not subject to an appropriately registered personal property security might still be sold for the benefit of creditors.

Other Obligations Not Affected

6.6 Nothing in this Act affects the other obligations a custodian might have because of the nature of the digital assets in their custody (for example, a digital asset exchange must hold the appropriate securities dealer licences to custody digital assets that are securities.)

This section confirms that this Act doesn't affect any other obligations a custodian might have. Custodians in the business of holding client assets might need certain securities licences, banking, or money remittance licences.

No Stamp Duty on Deemed Trusts

6.7 No person can ever be liable for any stamp duty, tax, or levy in respect of any trust deemed created under this section 6.

6.8 The trust deemed created under this section is valid and enforceable regardless of any statute, or principle of law or equity to the contrary.

Having deemed a trust to exist, we don't want state government stamp duty laws somehow levying stamp duty on the assets in the deemed trust.

7. Limited Liability of Developers

7.1 In this Act:

(a) **Software developer** means a person who writes, tests, or commits code that becomes part of:

(i) A decentralised public network.

(ii) A network contract.

(iii) A community smart contract.

(iv) A non-custodial wallet.

(b) **Non-custodial wallet** means a software application that allows a user of a decentralised public network to interact with the open-source code that comprises the decentralised public network's rules by means of private keys the user exclusively holds or controls.

7.2 Unless they otherwise agreed, a software developer is not liable in law or equity to anyone for any kind of loss, damage, or suit arising in any way from any open-source code they wrote, tested, or committed incorporated into:

(a) A decentralised public network.

(b) A network smart contract.

(c) A community smart contract.

(d) A non-custodial wallet.

7.3 7.2 does not apply to any damages, loss, or suit arising from:

(a) the operation or failure of any closed source code the software developer writes, tests, or commits.

(b) A developer smart contract.

(c) Any of the software developer's conduct that constitutes a crime or fraud.

There is a fringe view that developers of the code base of a code governed network should be treated as fiduciaries. This proposal emphatically rejects this approach.

If developers of open source blockchain projects were fiduciaries it would be debilitating and hopelessly centralising. It would mean developers of open-source code have greater liability than companies like Microsoft for source code that is never made public.

Instead, this section proposes to give software developers a decentralised public networks and smart contracts immunity from liability, except where they cause loss or harm because of closed-source code, bad faith, or criminal conduct. The section is necessary if Australia wishes to be a welcoming jurisdiction for developers.

8. Limited Liability of Oracles

Definitions

8.1 In this Act:

(a) **Oracle** is a person, computer, or decentralised public network that feeds off-chain data to a decentralised public network with the purpose or potential to influence transactions on the network.

(b) **Warrants the accuracy of the data** means:

(i) If the oracle is feeding data from a third party, it accurately reports the third party's data, not that the third party's data is accurate.

(ii) If the oracle is feeding data it owns, controls, or represents it has verified, it warrants the data is true, not just that it is truthfully reported.

Oracle Warranties

8.2 If the oracle is a person, that person warrants the accuracy of the data to all users of the network, subject to any lawful terms and conditions of service communicated publicly to the entire network.

8.3 If the oracle is a computer, the person operating the computer warrants the accuracy to all users of the network, subject to any lawful terms and conditions of service communicated publicly to the network.

8.4 If the oracle is multiple computers that comprise a decentralised public network, then no liability is possible because of section 1.4.

8.5 Nothing in this Act limits the oracle's liability for losses or damages caused through their criminal conduct, fraud, or gross negligence.

No Liability for Third Party Data Providers

8.6 Any third party from whom an oracle sources data is not liable in law or equity to anyone for any kind of loss, damage, or suit arising in any way from any network's use of that data, even if the third party was in any way aware of, or agreed to, the oracle's use of their data.

8.7 Section 8.6 does apply to the extent the third party's conduct constitutes a crime or fraud.

Some oracles feed data from other sources. They should be liable for the accuracy of their feed, but not warrant the accuracy of the source data. If the oracle is reporting what the BOM says the temperature is in Canberra, the oracle warrants that this is the temperature the BOM reports, not that the temperature BOM reports is the true temperature.

Some oracles feed data they own or represent they have verified. They should be liable for the truth of this data. (If the oracle is reporting that an RFID ear tag matches a live cow, the oracle warrants this is true, not just that someone says it is true.

People should be able to supply data to an oracle without being liable for how the oracle uses it.

To guard against manipulation and downtime, some oracles also run on decentralised public networks. Users of such a network should receive the same immunities as any other decentralised public network.

****End of Proposal****