

# ADT

## Australian Institute for Digital Transformation

Comments on  
Australian Treasury's  
request

27.05.2022

**Exclusive, Full and Limited Control  
Over Crypto Assets**

---

# CONTENTS

Intro

Permissioned vs Permissionless

Crypto Asset vs. Digital Token

Two types of control

- Single signature
- Multi-signature schemes

Licensing

## Summary

This paper raises an important issue that was not in the focus of the Australian Treasury's request for feedback and comments about "[Crypto asset secondary service providers: Licensing and custody requirements. Consultation Paper.](#)" The Consultation Paper refers to custodian safekeeping with regard to those who get "control over crypto-assets" while providing custodial and/or other commercial services, e.g., exchange, asset administration, etc. It is crucial to delineate custodians and other keykeepers (escrows, arbitrators, etc.), including those using certain multi-signature schemes. This paper presents various scenarios of digital asset control and explains potential risks to customers. The proposed analysis can be used to develop public policy on the variety of third party roles. It is suggested that third parties that gain *limited control* over crypto assets will not fall into a licence category, as well as parties that operate with non assets (other digital tokens). To range licence requirements the Australian regulator may want to introduce asset value thresholds, while deals with low value assets will be relieved from licence burden.

---

## Intro

The consultation paper of The Australian Treasury, "Crypto asset secondary service providers: Licensing and custody requirements," requested feedback and comments on regulations that should be imposed to regulate custodial and other safekeeping services that deem control of a third party over a user's crypto asset. However, the paper did not elaborate on variants of control, such as **exclusive, non-exclusive and limited**, and situations when it happens and hence the roles of trusted third parties in this market, e.g., **escrow services, arbitration**, etc. Delineation of control types with the context of technology specifics is crucial as it allows for building risk models and developing relevant regulations. Therefore, the core of the discussion is the **Risk Disclosure Protocol** which elaborates on risk issues that customers should be informed about concerning their crypto assets.

The distinguishing feature of a crypto asset is its reliance on the Digital Signature Algorithm which is a technique of Asymmetric Cryptography.<sup>1</sup> A user realises its ownership over a crypto asset through a cryptographic pair (private and public key). The asset record (digital token) is attached to a representation of the user's public key (which is referred to as an 'address,' a 'cryptocurrency address,' or a 'blockchain address'), while the relevant private key is needed to authorise a blockchain transaction, through the algorithm of digital signature.

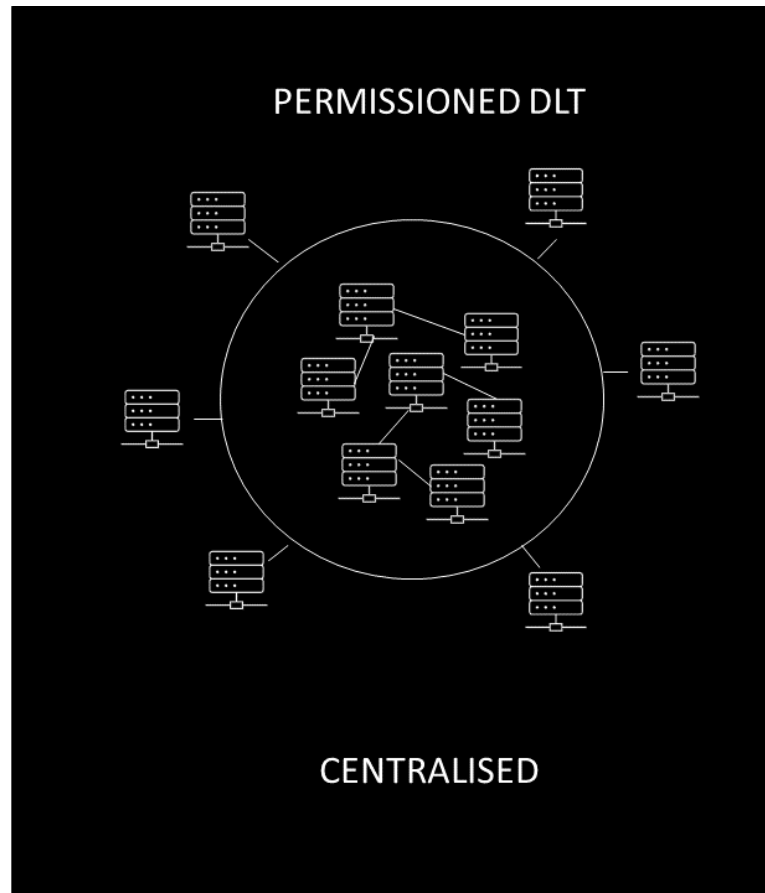
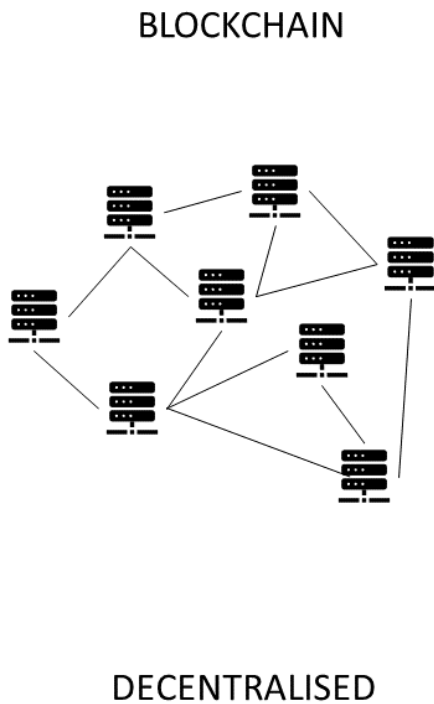
Additionally, it should be emphasised that cryptographic digital signatures form the technology of digital assets. At this point, the discussion cannot be technologically neutral as there will be no crypto assets without asymmetric cryptography. Thus, the following analysis unpacks features of this technology important for developing public policy, and the last section elaborates on how to design regulations around these specifics.

**It proposed that third parties that gain limited control over crypto assets will not fall into a license category.** However, they will have to comply with some CASSPr regulations, such as the practice of risk disclosure to their customers. It is also proposed that crypto asset as a property category is distinguished from a general concept of digital tokens. Not every token is an asset (for example, when used as a voting mechanism). Hence, the participation of a third party in any arrangement without a property interest will not be regulated. The regulator should also consider ranging license requirements based on asset value. For example, third parties that operate with assets total value of less than 1 million Australian dollars will not need a licence, or will be subject to a specific regime, e.g., in a regulatory sandbox.

<sup>1</sup> Also referred to as Public-key cryptography.

# Permissioned vs Permissionless

Before diving into types of control that custodians can exercise, it is important to outline types of technology that can deal with as the choice of technology can also constitute a risk to a crypto asset. This paper draws the attention of policymakers to centralised types of distributed ledger, as there are a lot of misconceptions around the word 'blockchain.'



Cryptoassets can be created in two types of distributed ledger technology (DLT):

- **on a public permissionless distributed ledger**, usually referred to as the 'blockchain,' 'public blockchain' or 'permissionless blockchain'. It is characterised by an unconditional, open and competitive type of consensus protocol<sup>2</sup>. The blockchain is built around its native digital token, usually called 'cryptocurrency'. The blockchain can have embedded (e.g., smart contracts) or third-party technologies for creating user digital tokens (crypto assets) as the second layer above the native token. The blockchain is characterised as an immutable distributed ledger.

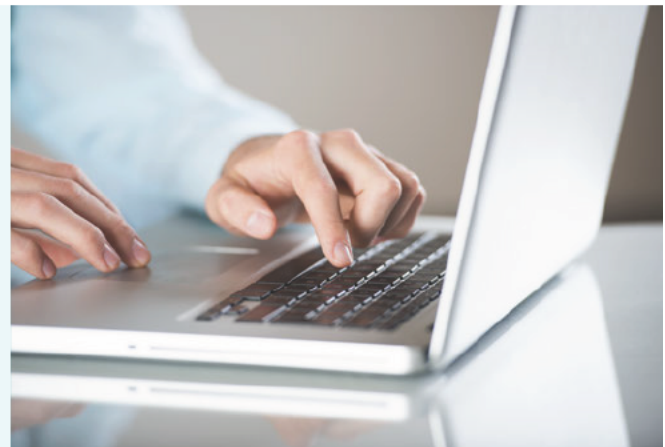
<sup>2</sup> Consensus protocol is the mechanism of how nodes of a DLT network synchronise and agree about the valid version of the ledger. In blockchains, nodes compete in block creating ('mining'), which gives them the right to rewards in cryptocurrency.

- **on permissioned or private distributed ledger technology (DLT)**, also rarely 'federated', 'enterprise' and 'cartel DLT'. The word 'blockchain' is also used in combination with the mentioned noun modifiers, though it is not academically correct. This type of technology deems the presence of a controlling party or parties. While the controlling parties can establish decentralised governance within their circle, such a network remains centralised towards users who are not members of the network. DLT may or may not have its native digital token. Also, it may or may not provide services for creating user crypto assets.

Variants of centralised DLT can constitute certain risks for crypto-asset owners, but controlling parties usually do not gain control over their private keys; hence, they do not provide safekeeping services. The controlling party (parties) in such a DLT can rewrite the ledger as it is not immutable, contrary to the public blockchain and misappropriate assets. Transactions can also be erased, so as the records of asset ownership. These aspects are crucial for developing public policy on technology providers.

### **CASSPr have a range of options:**

- **permissionless blockchain**
- **a third party controlled DLT**
- **its own controlled DLT**



A custodian, in its turn, can use this range of options: (1) permissionless blockchain, (2) a third party controlled DLT or (3) its own controlled DLT. In the latter scenario, the custodian would be both a technology provider and a key keeper (custodian), which constitutes the highest risk towards crypto-assets and should be considered equal to the conventional centralised technology.

<sup>3</sup> The paper "[Why 'Permissioned' and 'Private' are not Blockchains](#)" by O. Konashevych, SSRN (2019) explains that not every chain of blocks is a blockchain and concludes that it is academically incorrect to call centralised DLTs (permissioned, private, etc.) blockchains. Academic rigour dictates to say 'permissioned DLT' rather than 'permissioned blockchain.'

# Crypto Asset vs. Digital Token

To regulate crypto asset secondary service providers (CASSPrs) and as a part of the token mapping exercise, there should be an articulated difference between crypto assets and digital tokens. The first one is an economic notion, while the latter is a technologically one.

Each crypto asset is a digital token, while not every digital token is an asset.

Digital tokens can be used for voting and other non-property relationships. Mere creation and use of the digital token on DLT does not make it valuable. Therefore, the involvement of a third party does not create economic risks to the asset owner.

Generally, we should consider that the token is not an asset if it is not offered for an exchange with an asset (fiduciary currency, securities, precious metals, other crypto assets, or other commonly recognised assets) or manifested as a property interest.



## SIGNS OF A CRYPTO ASSET

- 1** Offered for an exchange with an asset
- or
- 2** Manifested property interest

# Two types of control

There are two distinguished techniques of control of a third party over a crypto asset:

- A third-party gains control over the private key
- A third-party gains control over one or more of the private keys controlling the crypto asset

There are different degrees of control over a crypto asset:

- a full exclusive
- a full non-exclusive
- a limited control

The following table schematically shows the relationship between these two types. It should be noted that the single signature algorithm always gives full control (exclusive or non-exclusive though).

Types of signature \ Types of control		Types of signature	
		Single signature	Multi signature
Exclusive	✓	✓	
Non-exclusive	✓	✓	
Limited	✗	✓	

## Single signature

In the single digital signature algorithm, only one private key can authorise a transaction with a crypto asset. Although the ability to copy and share the private key extends how many persons can have full control over the assets. Besides, copying of the private key can happen due to unauthorised access (hack or leakage of the key). The loss of the only key can cause an unrecoverable loss of the asset. If a custodian exclusively owns the private key, and the asset owner does not have a copy of it, such key keeper constitutes a maximum risk level.



Suppose the key keeper and the asset owner both have the copy. In that case, the custodian has non-exclusive access to the asset but cannot be fully responsible for the crypto asset, as the key can be compromised on the end of the asset owner, which would be beyond the custodian's control.

There are no cases when a key keeper gains limited control over an asset through a single private key. The private key in the single signature scheme unconditionally provides full control. A third party that controls the private key in the single signature scheme can provide commercial services to a formal owner by intermediating access to the relevant asset.



## Multi-signature schemes


There is more than one private key in a multi-signature scheme (in professional jargon, also known as the 'multisig').

Mathematically a multi-signature scheme is communicated as *n-of-m*, where *n* is the number of keys required to authorise a transaction, and *m* is the total number of available keys in the scheme. *n* is always less than or equal to *m*.

Such schemes can provide full exclusive, non-exclusive access or limited control over its relevant crypto asset. Multisig is often used to provide limited control of a third party to ensure they can perform their function (custodian, escrow, arbitrator, etc.). Exclusive full control is also possible when the third party possesses the controlling number of keys in the scheme. For example, suppose a third party is a custodial company. In that case, different employees can have their keys to ensure that one employee cannot unilaterally transfer a crypto asset. At the same time, the owner retains full exclusive control over the asset. Therefore, for the sake of regulation, this should be regarded as a single exclusive scheme, a bit more secure perhaps.

In a non-exclusive multi-signature scheme, such a third party will have that number of keys that give them an ability to unilaterally commit a transaction, but other scheme partners (an interested party or another third party) also have this possibility.

A multi-signature scheme can be used solely by an owner, for example, to ensure access to a crypto asset from different devices, or to ensure a multifactor authentication when the participation of more than one signing device is controlled by the same owner is needed to authorise a transaction. A multi-signature scheme can be used by co-owners of a crypto asset. For example, partners can use a non-exclusive multisig to ensure access from their own devices. They can also design a scheme which makes it impossible to unilaterally dispose of a crypto asset, but for instance, through the consent of the majority of owners. Parties can design a scheme that will require all the co-owners to agree to a transaction. Since no third parties are involved here, there are no reasons to regulate it.



---

Multi-signatures can be used in relationships between interested parties<sup>4</sup> with third parties, such as custodians, escrow, arbitrators, etc. The involvement of a third party must be pre-designed in such a scheme and agreed upon with interested parties. A custodian would normally mean a third party that provides safekeeping services. Such a provider would accept and execute orders from the crypto asset owners.

An escrow in a multi-signature scheme provides intermediary services for counterparties. A classic example would be a situation when the seller dispatched the product, and until it arrives at the buyer's, the payment (in crypto asset) is stored on a 2-of-3 multi-signature address. If the buyer is satisfied with the product, the seller and the buyer mutually authorise the transfer of the payment in favour of the seller. If the counterparties have a dispute, the escrow with either party can release the funds, as only two digital signatures are needed. Therefore, the escrow cannot fully control a crypto asset and unilaterally dispose of it. If the escrow's private key is compromised, it can increase the risk of an unauthorised transaction. It is important that the escrow bears the responsibility to notify counterparties if the escrow's private key has been compromised.

An arbitrator should bear similar responsibilities. There is not much difference between the escrow and arbitrator. The arbitrator would be a better role name in some specific situations. For example, an escrow can perform an independent technical function of key keeping, with an obligation to sign a transaction when a disputing party presents a legally valid dispute resolution. Therefore, an arbitrator would be another third-party that does not physically control the crypto asset but has formal authority in dispute. It can be a judge (of a court) or a private arbitrator.

A multi-signature scheme should be emphasised as the technology does not define roles, such as an owner of the asset, a custodian or an escrow, in such an arrangement. The relationships between a crypto-asset owner and a third party or parties (that do not have an interest in the asset) should be defined by an agreement. The absence of contractual relationships would mean that the parties of a multi-signature scheme have an equal property interest.

The escrow function for crypto assets using a multi-signature scheme is different from conventional escrow because the escrow would keep money or property under its full control. Therefore, it cannot be regulated the same way as fewer risks are involved.

<sup>4</sup> The phrase "interested parties" covers both situations when parties have equity interest in a crypto asset, such as co-owners, and opposite interests, such as counterparties in a purchase contract.



There are several important characteristics of multi-signature schemes.

Depending on the number of third parties, there can be: **sole** (one third-party) or **shared** control (multiple third parties).

Depending on the involvement of an interested third party, there can be: **non-delegated** participation, i.e., an interested party has a key or **delegated**, i.e., an interested party does not have a key.

There can be designed three basic types of decision-making/controlling schemes in a multi-signature arrangement:



### **Full control**

either party can authorise a transaction



### **Collective control**

a type of limited control where several keys are required to authorise a transaction (for instance, a majority)




### **Unanimous control**

a type of limited control where all the keys are needed to authorise a transaction.

The loss of at least one in the unanimous arrangement will make a crypto asset inaccessible, while theft of one or more keys but one, will not lead to misappropriation of the asset.

### **Multi-signature schemes with an exclusive control**

In some multi-signature schemes, a third party can retain exclusive control over the asset. It is possible that such a third party will get access to the keys needed to gain control over the asset. Therefore, a limited or non-exclusive control will become a full exclusive control. Such a third party can enquire keys or acquire entities that participate in the scheme.



---

For example, the scheme can have three companies that provide arbitration services in a multisig scheme with two counterparties (4-of-5 multisig scheme). Acquiring by one of the companies at least one of two other companies will give a formal majority in dispute resolution by such arbitrators. If such third party acquires an interested party in the dispute (hence, acquires 4 of 5 keys), such a third party gains exclusive control over the asset.

### **Multi-signature schemes with a non-exclusive control**

There are several schemes where a third party has non-exclusive access and can unilaterally commit a transaction while the owner (or co-owners) of a crypto asset can authorise a transaction without such a third party. 1-of-n is a basic non-exclusive scheme where either key of a number of keys can authorise a transaction. For instance, a 1-in-2 scheme will have a total number of two keys, and either of them will have full control over the asset.

The responsibility of a third party is limited in a non-exclusive scheme because the other party (parties) can compromise the crypto asset. Hence, such a third party would not be responsible for that.

The difference from mere copying the key in the sole scheme is that in certain algorithms, it is possible to identify who exactly participated in transaction authorisation; therefore, it might be possible to determine whether the third party was responsible for it.

The first Bitcoin multi-signature script was designed to reveal signatories. Bitcoin Sigwit protocol and the use of Schnorr's multi-signature scheme (MuSig) made it impossible to determine signatories of a multisig scheme by referring to blockchain data.

### **Multi-signature schemes with limited control**

The scheme as mentioned is used between interested parties and a trusted third party (parties).

m-of-n is its basic formula, where one or several m keys are possessed by a third party or third parties. In this scheme, the interested party or parties may or may not have m number of keys. The arrangement can require a collective or unanimous decision to authorise a transaction. The nature of the technology they use will dictate an extension of the responsibility of third parties towards asset security. They cannot be fully responsible for an asset if they use a scheme that does not allow to determine which key participated in transaction authorisation. Such schemes impose larger risks to the asset.

# Licensing

It is proposed that a third party that gains a full exclusive or non-exclusive control will fall under the licensing regime. As part of their obligations under the license, the third party will need to provide full disclosure of risks to an interested party before committing to service, and also immediately each time risks change.

A third party with limited access to a crypto asset through participation in a multi-signature scheme in which such a third party cannot unilaterally authorise a transaction will not need a license but will also be obliged to provide full disclosure of risks to an interested party and update when risks change.

Therefore, the following table presents the **Risk Disclosure Protocol** that advises on the issues an interested party should be informed about:

1. A third party must declare its specific role or roles and responsibilities in a safekeeping arrangement.
2. The third party must declare what such party knows about how many interested parties are in the arrangement and their relation to the crypto asset, e.g., an owner, a counterparty (buyer, seller, etc.). The third party must inform an interested party what relationship such a third party has with other interested parties concerning crypto assets and whether such a third party has a conflict of interest.
3. Can the third party exclusively authorise a transaction with the crypto?  
Exclusive is such control that allows the third party to unilaterally authorise a transaction while no one else can authorise or block its authorisation. It is still exclusive if the third party internally uses a multi-signature scheme in which the keys are shared among employees of such a third party. Such a scheme can be used for security and backup reasons.
4. Can the third party unilaterally authorise a transaction with the crypto asset? Unilaterally means no one can block it by non-authorising, but if there is at least anyone else who can authorise it, it is a non-exclusive control.
5. How many third parties are involved in the safekeeping arrangement? What are their roles and responsibilities? What is the scheme of authorisation of a transaction? The third party must declare if any other participating party is dependent on it or affiliated with it, and each time such a dependency or affiliation happens during the arrangement.
6. Does the safekeeping arrangement involve a single signature scheme? Does the interested party possess a copy of the private key?
7. Does the third party use a multi-signature scheme? For what purposes? How many private keys are in the arrangement, and how many are needed to authorise a transaction? How many keys control the third party? Does the interested party possess a private key in such a scheme? Who else possesses a key? The third party must disclose the protocol and/or standard of the multi-signature scheme, including whether the arrangement allows to determine which key participated in a transaction authorisation. In a multi-signature scheme where the third party uses a multi-signature scheme for internal purposes, retaining an exclusive control, such a third party, for security reasons, does not need to disclose who exactly possesses the keys.
8. The third party must advise how the interested party will be informed if the safekeeping arrangement is compromised (loss, theft of a private key and so on).
9. The third party must advise how the interested party can inform the third party about the compromise of the arrangement.
10. The third party must inform about other circumstances that influence risks to the crypto asset.
11. The third party must inform each time when a risk changes.
12. The third party must inform whether the technology where the crypto asset resides is decentralised (permissionless) or centralised (permissioned), and inform who controls such a centralised ledger, including whether such a third party has a certain level of control over such a ledger.

CONTACT: Alex Konashevych

Executive Director

Ph: [REDACTED]

email: [REDACTED]

[www.aidt.org.au](http://www.aidt.org.au)

ADT