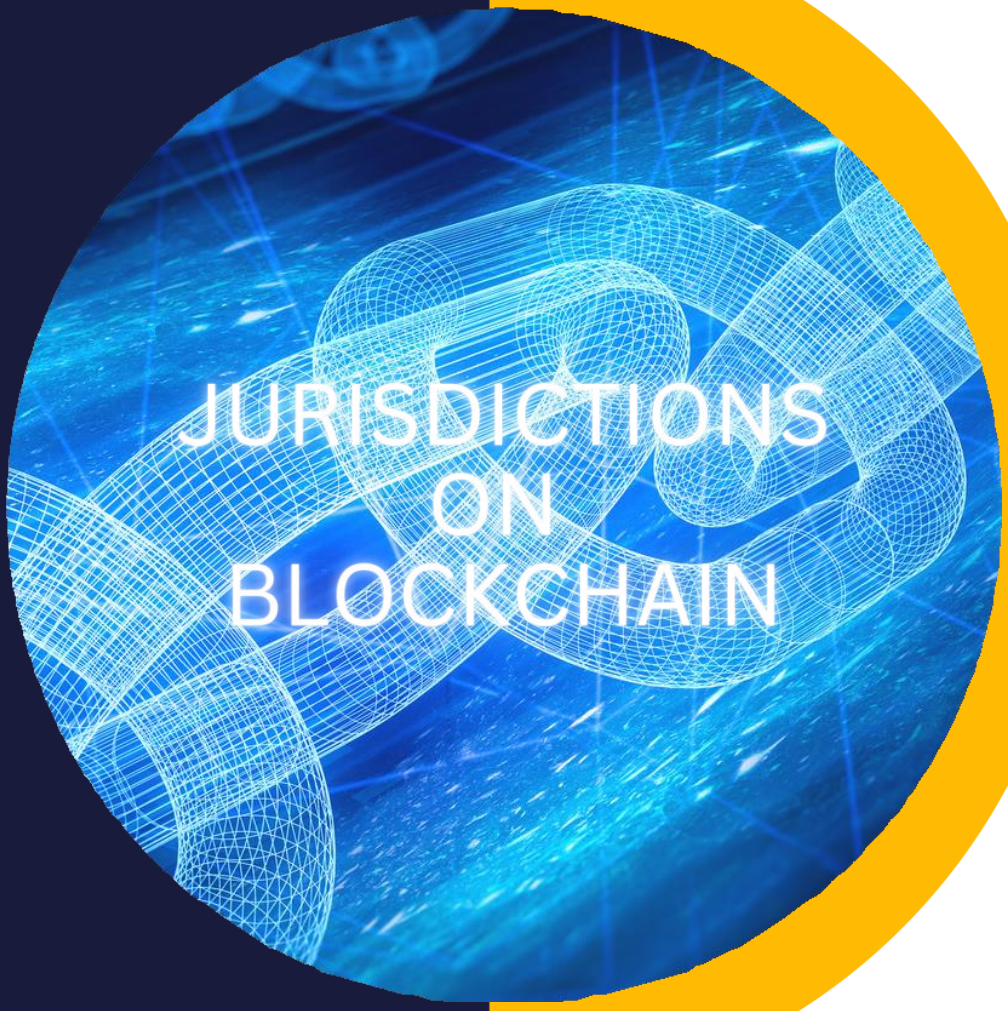


MARCH 2023

RESPONSE TO AUSTRALIAN TREASURY'S CONSULTAION PAPER

TOKEN MAPPING

PREPARED BY: DR OLEKSII KONASHEYVCH

To

DIRECTOR - CRYPTO POLICY UNIT
FINANCIAL SYSTEM DIVISION
THE TREASURY

03.03.2023

Dear Ms Raman,

About me

My name is Dr Oleksii Konashevych. I have been researching on blockchain and fintech since 2016 and completed my PhD thesis on blockchain. In 2021, I spoke before the Australian Senate Committee responsible for blockchain and fintech issues. I presented the results of my academic research which then laid down as a part of the Committee's recommendations to the National Cabinet, specifically to consider launching a pilot withblockchain land registry (see further details in the last section of this paper 'About author').

Summary

After studying the Commonwealth Treasury's Token Mapping Consultation Paper, I would like to address some of the consultation questions and raise several issues.
In attempts to regulate the crypto industry, some countries imposed unnecessary bureaucracy that could have been avoided. Fintech innovations appeared as a response to inefficient institutional financial systems and regulatory environments in the first place. Thus, stifling it using traditional bureaucratic methods does not make this industry better. Liechtenstein is an example of introducing crypto regulation to attract innovations and investors from all over the world. They ended up having a conventional registry and slow bureaucratic procedures. After almost 3 years of operation, as of today, there is only 26 licensed providers in their state registry.
Australian regulators and lawmakers may want to adopt a more competitive regulatory environment. The declarative principle for obtaining authorisation (financial license) would allow entrepreneurs to launch innovations much faster than the full-scale licensing. Such a declaration in digital form would involve a disclosure (as per established requirements), selection of a relevant risk-based licence tier (normally, based on turnover and volume of liability), and using standard smart contract solutions or submission results of auditing, and a financial guarantee (collateral) or liability insurance when needed.
It is envisioned that providers of financial products and services can upgrade their licence tiers with the growth of their business. The risk-based approach in licensing would address the problem of unproportioned requirements for businesses of different scales and the discretionary power of the regulator. Exhaustive requirements for starting a licensed crypto business will create certainty and clarity for all industries looking into the direction of Fintech innovations. Besides, simplified rules can also eliminate expenses on legal support.
In academia I have been working on the concept of Jurisdictions on Blockchain, i.e., technology and methods aimed to address regulatory compliance and ensure presence of the authorities in the digital environment using standard smart contracts (making them legal smart contracts) and smart laws.
Section I of this paper addresses the risk-based licensing concept. Section II elaborates on the concept of Jurisdictions on blockchain followed by Section III, which discusses several issues spotted in the definitions and terminology of the Treasury's paper. The last section is about the author of this paper.

Risk-based approach

1.1. Token Mapping Consultation Paper refers to risks (page 5) associated with the crypto industry and emerging technologies. Would it be correct to say that the future crypto regulation aims to address or mitigate risks? If so, the token mapping could pay more attention to specifying these risks when describing the 'functions' of crypto technologies and intermediated services (Q2 - Q3).

1.2. I propose a method of declarative principle for licensing financial services and products. Asset-wise speaking, there are two types of risks for an end-user: (1) technology imperfection and (2) dishonest or unscrupulous behaviour of intermediaries (intermediary risks).

1.3. Token Mapping introduced "public token systems" and "intermediate tokens systems". The problem is that both concepts inevitably deal with two components: (1) a hosting network and (2) a blockchain-based application. Each one has its own risk, which is partially communicated in the paper but requires more clarity.

1.4. Permissionless public networks (which are generalised under the term "public crypto networks" are distinguished by their open competitive nature. Decentralisation in the network is a dynamic state, i.e., at any given time the network can be either centralised or decentralised. There is always a possibility that, for example, Bitcoin, can become centralised, i.e., intermediated and exclusively controlled. The distinguishing feature of such a network would be its **open competitive consensus mechanism** where anyone can become a member of such a network and participate (compete) in creating a cryptocurrency that is added to the ledger in the form of sequencing blocks, that can contain transaction data. Sometimes it ismisunderstood that members provide services of recording transactions as their primary function. A node can create a completely empty block with no transactions, ignoring all pending user transactions in the mempool (a communication protocol and storage where transactions wait to be included in a block).

1.5. Intermediated networks are not fully discussed in Treasury's paper. Usually, intermediated/centralised networks are characterised as "permissioned" (only specific members are allowed to perform validation and data creating functions) and "private" (which indicates whether transactions are publicly available or not). Their centralised nature is usually pre-designed and remains so throughout their life span. The database (ledger) in such a network is not immutable, blocks can be deleted and rewritten. On the other hand, any open consensus competition network can also become intermediated (centralised) bona fide, i.e., by virtue of competition as per the protocol. This is a risk that should be clearly disclosed to retail customers of financial products and services.

1.6. It should be noted that disintermediated networks mostly provide functions for end-users through operating members (nodes), which is also an intermediation. But speaking in terms of their open nature, every user retains a possibility to record their transaction in the shared database (by 'mining' a block, i.e., adding new data to the shared database) if nodes for any reason decline to provide such a service. At the bottom line this is the distinctive feature of a public crypto network.
Whereas, in the permissioned networks, those who control it have a discretionary power to authorise data creation, meaning end-users cannot commit a transaction without an operator (intermediary). Therefore, permissioned networks are closer to traditional finances where, for example, clients cannot make records themselves in the bank's ledger.

1.7. Permissioned networks can be a consortium - a pool of controlling nodes, and their relations within this consortium can be decentralised and disintermediated. At the same time, for external users, it will always be a centralised system if such a system is offered for external use beyond such a consortium. Such a network can have signs of a cartel. Therefore, antitrust laws are applicable here.

1.8. Risks of intermediation of a network translate risks on applications on such a network. The application can be disintermediated but the network where the application is hosted can jeopardise its permissionless nature if it is controlled by a predefined party or parties, i.e., intermediated.

1.9. This discussion shows distinction between two components of token systems: (1) distributed ledger networks as infrastructure solutions for applications and (2) applications based on these networks. Each of them can be intermediated or not. This knowledge enables more precision in identifying risks for end-users.

1.20. There can be introduced different tiers for licensing similar activities. For example, a crypto exchange with a turnover of 1 million dollars constitutes fewer risks than an exchange with 10 million dollars.

1.21. Licensee developing its business model selects risk levels admitted in their business. Therefore, the regulator can establish different requirements depending on the licensee's business model and chosen technology.

1.22. Using the word 'blockchain' may mislead the average user, as the operators arbitrarily use this word towards all sorts of technologies, creating the impression that such technology ensures a certain class of security. For example, a custodial wallet through which a service operator controls users' private keys will constitute the same risk as a non-custodial wallet (the user' exclusively controls the key) but operated on a private ledger solely controlled by such an operator.

1.23. There are three degrees of control over the asset through the mechanism of ownership (normally ensured through public-key cryptography):

Full non-exclusive - when a service provider technically gets the ability to commit any transaction with the asset;

Exclusive - when the service provider has full control over the asset, the user does not have direct (independent) access to the asset, and such access is mediated through such a provider; and

Limited - when the provider cannot solely commit a transaction but needs a user or another independent party. Some multi-signature schemes provide limited access.

Full and Exclusive constitute **the highest risk** towards an asset, as the custodian can misappropriate funds or commit an unauthorised transaction which can be irrevocable in an immutable ledger.

1.24. Escrows can provide dispute resolution services under multi-signature schemes that technically restrict their sole control over the asset. Thus, such a service does not constitute an equivalent risk to those fully controlling private keys in custodial wallets. Therefore, I would separate custodial services with full and exclusive access and such services as escrow and arbitration in which the provider is **technically limited** to commit a transaction solely.

For example, Alice sends the product to Bob. Bob sends the cryptocurrency to a 2-of-3 multi-signature address as the payment. The address is controlled by Alice, Bob and an independent escrow, Chuck. If Bob gets the product, Alice and Bob will sign the transaction and release the funds to Alice. But if they have a dispute, Chuck will sign a transaction with either side.
Also, this scheme can have Judy as a private arbitrator or a judge. And Chuck, in this scheme, will play only a technical role of the key keeper but will follow the legal instruction of Judy.

1.25. The second group of risks arises from the use of a ledger technology itself. The provider of custodial services can be an operator of the ledger at the same time or use a ledger operated by third parties. The ledger can be intermediated (closed consensus). In either case, the ledger is not necessarily secure and immutable. Future regulation obviously should not regulate operators of ledgers or ledger networks, but the legislature should lay the responsibility on custodians, stablecoin issuers and exchanges (or else), as they eventually choose which technology to rely on.

- Custodial providers choose which ledger technology to deploy their custodial wallets.
- Stablecoin issuers choose which ledger to create their coins.
- Exchanges decide which digital assets can be admitted for trade on their platforms.

It is proposed that all licensees must publicly disclose all the risks and keep them up to date in their everyday activities. Disclosure requirements should oblige a licensee to explicitly answer whether ledger technology is public/permissionless, or private/permissioned. If the latter, they should specify the list of members, consensus mechanism and governance model.

1.26. For exchanges as well as for other licensees, it is proposed to introduce alternative tiers using a declarative principle. Under this principle, the regulator approves an application without actual expertise (only formal verification) when it contains the applicant's statement of satisfying all the requirements of this licence, and if such an applicant:

1) provides exchange within volume up to $10M (for example) daily; and
2) guarantees its liability by:
a) having insurance coverage of its provided by an Australian insurance company, or
b) having a financial guarantee provided by an Australian financial or banking institution of respective volume.
3) Uses technical standards recognised by the regulator (in this case, the applicant declaration that it uses some specific standards) or submits a technical audit report.

Volumes and respective tiers can vary (for example, volume/guarantee: 1/1 10/10, 100/100 million dollars and so on) up to some amount, after which the licensee shall obtain the full licence. For the full licence, the Regulator will have discretionary power to establish requirements, while the legislature will establish simple tiers.

2.1. While working on a new generation land registry system on blockchain in my academic research, I introduced a 'Jurisdiction on Blockchain' concept. Even though it was designed for land title rights (title tokens), it can be used broadly for any rights and interests because the legal issues that it addresses are similar:

- regulatory compliance; and
- enforcement, i.e., transferability of a right having no consent of an owner (for example, in the result of a dispute in a court) or no technical access (death of a token owner, loss of private key, etc.).

2.2. Custodial services with exclusive or full control over the asset by a third are risky as they imply the discretionary power of such an intermediary. It is unlikely that such a solution can find mass use (considering that better designs are possible), or at least it is not better than how rights are managed and services are provided in traditional industries.

2.3. Jurisdiction on blockchain on blockchain offers a sustainable way of designing applications on blockchain. The principles of their design imply two basic things:

- the owner retains full exclusive control of their asset through the mechanism of cryptography (private and public keys);
- the application is designed in a way that enables addressing legal issues by third parties. Thus, it has two components, i.e., requirements for an application (smart contract) and a third party with the authority to perform functions to resolve legal issues.

2.4. Legal issues must be addressed through the existing procedures (a dispute in a court, an inheritance procedure by an administrator or executor etc.). While the directions find their implementation in specific blockchain transactions enabled in complaint blockchain applications.

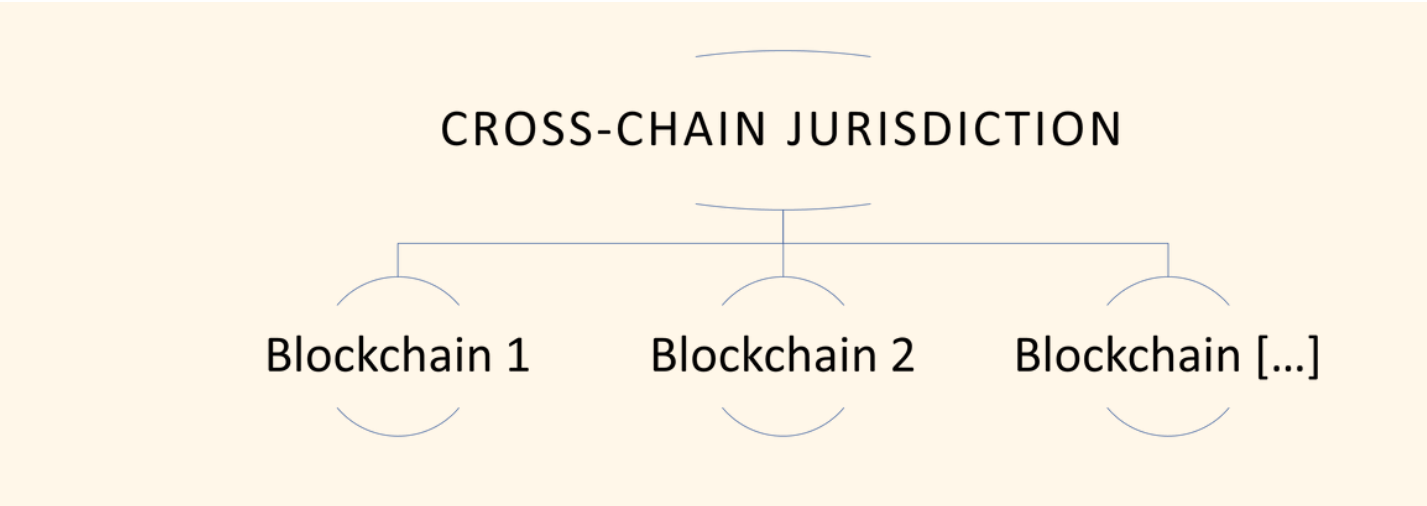
2.5. It is a matter of how the government can implement it in the range of possible solutions. For example, a court can have its digital presence and cast its decisions through blockchain transactions, or the court acts conventionally but an authorised person implements paper- based rulings in transactions on blockchain. The basic principle remains the same, i.e., jurisdiction on blockchain would require the following requirements (Smart Laws) in designing smart contracts and applications on blockchain that enable validation and invalidation of assets through the means of authorised third parties (Digital Authority).

2.6. The Jurisdiction on blockchain has two modes: jurisdiction as a filter - when applied to any blockchain, it shows which transaction is valid or invalid, i.e., whitelisting, and blacklisting - an authority can invalidate any transaction or a smart contract even if it is not included in the perimeter of the Jurisdiction (designed without the use of the adopted requirements). Whitelisting and blacklisting can be combined.

2.7. Standardisation is on the way to designing Jurisdiction compliant applications. And a service provider would need to simply use the existing tools and declare to obtain the licence.

2.8. Custom-designed applications to be compliant would need technical expertise (audit) to be admitted to the Jurisdiction.

2.9. Jurisdiction on blockchain is conceptualised as an **interoperable** solution where end-users and service providers freely decide within the range of admitted blockchain networks. It will ensure market competition of technologies.



2.10. Jurisdiction on blockchain makes governance and public services transparent as the decisions of the authorities must be executed as blockchain transactions, otherwise, they would not enter into legal force. It ensures that the source of knowledge about the legal validity of an asset is always tied to the digital asset as blockchain transactions that indicates its validity/invalidity. No off-chain hence unpublic decisions by authorities are possible towards the digital assets.

2.11. Specifically addressing Q6, it is worth noting that obviously 'backed', 'wrapped', and 'pegged' notions are not legal terms but evolving marketing parlance. A digital token is a record on a distributed ledger. It has a legal and an economic meaning through a deed or an agreement. There can be only two types of such records from a legal perspective: (1) a record of ownership, which is not a promise of something. It is an actual leger record that indicates a title (a bundle of rights), similar to a paper certificate or another type of an ownership record, transfer of which would convey the right; (2) a record of a right or interest in someone's property (property in its widest meaning), that can be a legal promise. Different types of property might need separate regulation, for example registered rights (real estate, vehicles, vessels, aircraft, corporate rights, some types of intellectual property), therefore, there cannot be universal crypto regulation for "wrapped" assets.

2.12. For example, if introduced in a jurisdiction as a legitimate way to exercise land title rights, a title token would be the record of ownership transferable in a smart contract (which would not need any further registration elsewhere, as blockchain is a registry). Or a property security token representing a token holder's interest to receive a portion of rental income from the property. The transfer of such a token would mean a transfer of this right (not the title right).

3.1. Treasury refers to physical tokens. However, it would be an accurate parallel. Even though the digital tokens have much in common with their physical vis-à-vis, that comparison would reflect the real nature of the digital asset. A transfer of the physical token is not necessarily traceable and/or documented. Whilst the nature of the digital asset presumes that it is a record in a cryptographically protected database (the blockchain is a kind of database, after all), its transfer is natively documented as a transaction on blockchain – i.e., as a record of transfer in that database. The transfer of a private key cannot be considered an adequate transaction practice, as it presumes the loss of exclusive ownership because the one who copies the private key and gives it to an acquirer still retains control over the asset.

3.2. Section 90 discusses **cryptocurrency networks** (for example, Bitcoin) and **general purpose networks** (for example, Ethereum). It should be noted using the word "primary" is correct in definition networks but not fully accurate. The cryptocurrency network is primarily used to operate with a native token (cryptocurrency) but not necessarily exclusively. All general purpose networks are derived from the function of a crypto network that lets users publish arbitrary data in the blockchain. Exploration of this function in Bitcoin and other first-generation blockchain networks eventually led to the idea of creating applications (of general purpose) on blockchain. One of the examples would be the OMNI Layer protocol which is effectively a set of development tools and techniques that allows the creation of token applications on Bitcoin(and Bitcoin-like systems).
The following discussion in section 91 is irrelevant as it insists that the crypto network is not designed for general applications. It is correct to say that it was not intended, but their design allowed the creation of applications, starting from the very first block in the Bitcoin blockchain.

3.2. Section 91 specifies "smart contracts considered" in this paper. For unclear reasons, the authors exclude discussion of smart contracts on Bitcoin and other similar systems, according to Nick Szabo (who was the author of this concept) Bitcoin's scripts are also smart contracts. To add, applications built upon such a network, for example, using the mentioned OMNI Layer, are also smart contracts, according to their initial meaning. Worth noting that Tether's USDT stablecoin as a multi-ledger token system relies on Bitcoin Cash. USDT tokens are built onBitcoin Cash using the mentioned OMNI Layer.

Nick Szabo, an American computer scientist, is thought to have first used the term smart contract in an article in 1994. He wrote (Szabo, 1994):

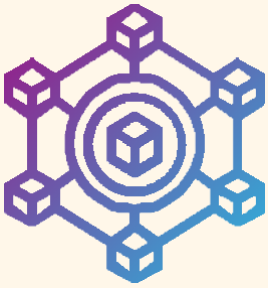
A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart-contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.

3.4. Sections 155 to 157 discuss forks. However, it is worth distinguishing natural (normal) forks that result from mining competition as bona fide, not a malicious act, as the 156 communicates.
Here applies the basics of public blockchain - the rule of the longest chain. The longest chain is the winning chain that nodes normally would keep as the correct version of the ledger. Nodes that have a different version of the chain, finding out that it is shorter than another one, drop that short chain (orphaned blocks).

Hard forks, the second type of forks, can be enabled in the result of a willing act of creating a ledger with a different protocol. Nodes that follow the original protocol keep the initial version of the chain. The forked blockchain starts creating blocks according to new rules. Such a fork, as correctly mentioned in the paper, can be operated even by one node.

A 'Soft fork' would be a change of the protocol that does not lead to a network split.

FORKS



HARD
new network

SOFT
the same network with modified functions

NORMAL
orphaned blocks

OLEKSII KONASHEVYCH, PHD

Joint Ph.D. in Law, Science and Technology (2020) in the European international program "Erasmus Mundus" led by the University of Bologna (Italy) and partnering universities.

Fields of research: Jurisdictions on blockchain, Blockchain Land Registry, the use of blockchain technologies in the public sector and real estate, digital identity and self-sovereign identity.

In 2021, based on my academic research I made a submission to the Select Committee on Australia as a Technology and Financial Centre of theAustralian Senate and spoke before the Committee presenting the concept ofa Blockchain Estate Registry. The Senate recommended the National Cabinet to consider launching a blockchain pilot with land registry (See Sections 5.34 - 5.36 and 7.59 of the Report in April 2021).