Blockchain Australia

Blockchain Australia - Submission to Attorney General's Department

Reforming Australia's anti-money laundering and counter-terrorism financing regime

Paper 4: Further information for digital currency exchange providers (DCEPs), remittance service providers and financial institutions.

Paper 5: Broader reforms to simplify, clarify and modernise the regime

28 June 2024

Blockchain Australia

c/o Hall & Wilcox
L 11 South Tower, Rialto
525 Collins Street,
Melbourne VIC 3000

28 June 2024

Attorney General's Department

Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

cc: economiccrime@ag.gov.au
Subject: https://consultations.ag.gov.au/crime/reforming-aml-ctf-financing-regime/

Table of Contents

Blockchain Australia

1. Executive Summary

Blockchain Australia, and its members, emphasise that Australia is currently behind global FATF standards in several key areas related to anti-money laundering and counter-terrorism financing (AML/CTF). It is imperative that changes are made to Australia's regulatory framework to ensure alignment with best global practices and most importantly, effectively address the new evolving threats of financial crimes.

Consequently, Blockchain Australia advocates for the following primary changes to be made, further detailed in the responses:

1. **Expansion of Definition of 'Digital Asset' and Scope of AML/CTF Legislation:** The term 'digital asset' should be amended to include NFTs and stablecoins with appropriate carve-outs, as noted below, to align with global standards, such as those from the Financial Action Task Force (FATF).

2. **Travel Rule Requirements:** Based on experience cited by global DASP members, DASPs will require a 24 month transition period to implement operational procedures for Travel Rule compliance.

3. **IFTI Reporting Requirements:** Current reporting requirements should be amended so that only essential information is captured, and require collaborative work between AUSTRAC and DASPs to provide an integrated secure reporting option for DASPs with a transition period in line with the Travel Rule.

4. **Amendment to Tipping Off Offence:** Legitimate sharing of information within business groups and regulatory bodies should be allowed. Consideration should be made to private-to-private information sharing.

2. Blockchain Australia Overview

Blockchain Australia is the peak industry body representing Australian businesses and business professionals participating in the digital economy through blockchain technology. Blockchain Australia encourages the responsible adoption of blockchain technology by the government and industry sectors across Australia as a means to drive innovation and create jobs in Australia.

This submission is made by Blockchain Australia, in collaboration with its members and industry stakeholders. Blockchain Australia gives special thanks to the following members for their role in hosting the policy response sessions and contributing to this submission:

- DCE Working Group Chair - Tom Bennett, Head of Operations, Swyftx
- DCE Working Group Co-Chair - Michi Chan, VP Regulatory Compliance, Crypto.com
- DCE Working Group Board Sponsor - Jackson Zeng, CEO, Caleb & Brown
- DCE Working Group Secretary - Paul Derham, Managing Partner, Holley Nethercote
- Digital Assets Working Group Secretary - Michaela Juric, Head of Blockchain and Digital Assets, Novatti
- Digital Assets Working Group Board Sponsor - John Bassilios, Partner, Hall & Willcox

Please direct enquiries to:

Amy-Rose Goodey
MD, Blockchain Australia

argoodey@blockchainaustralia.org

3. Methodology

In response to the Consultation Paper, Blockchain Australia has gathered input from our member base. Blockchain Australia has a membership base of 130+ businesses, 28 of which are classified as Digital Currency Exchange (DCE) members. These members would meet the definition of a "Digital Asset Service Provider" set out in the current proposal in the Consultation Paper. Additionally,

We extended an invitation to all of our DCE members to contribute to a collective response to this consultation. Additionally, we welcomed participation from other members who have interests in the regulatory framework surrounding Digital Assets. We have a DCE Working Group and a Digital Assets Working Group, and we thank members for their participation across both Working Groups.

Through this inclusive approach, we garnered insights from 70+ organisations over the course of four video conferences and asynchronous written input, which has been incorporated into this response for the Attorney General Department's consideration.

4. Recommendations to Paper 4: Further information for digital currency exchange providers (DCEPs), remittance service providers and financial institutions

4.1 Amending the definition of 'digital currency'

It is imperative that the scope and application of laws and regulations concerning digital assets are more clearly defined. This is imperative to respond to the growing variety of digital financial instruments used for transactions and will ensure Australia's alignment with global standards.

Topic	Response
Expanding the range of regulated digital currency-related services	**a. Do you consider that the current term and associated definition of 'digital currency' is appropriate? What alternative terms outside of 'digital asset' might be considered, and why?** Overall, the rationale for the proposed change in terminology to 'digital asset' appears reasonable as it is more inclusive of NFTs and other financial instruments. In the spirit of aligning Australian standards with the FATF, we propose that the Attorney-General's Department consider adopting a more globally-used taxonomy. For example, FATF uses the term 'Virtual Assets' and refers to digital currency related service providers as 'Virtual Asset Service Providers' (VASP). In relation to asset coverage, we believe that stablecoins that are used as a form of payment should not be included as a digital asset. Along with CBDCs, these stablecoins should also be considered as 'money'. We urge the Attorney-General's Department to consider any potential unintended consequences of the amendment. For example, the potential tax implications such as CGT if stablecoins were to fall under the category of digital assets. Recommendation We propose that the Attorney-General's Department adopt a change in methodology and align terminology with a globally relevant

Topic	Response
	taxonomy. We also recommend that terminology also align with Treasury's work on Digital Assets with respect to its Digital Asset Platforms and Payment System Modernisation projects
Scope of Regulation on NFTs	**b. How should the scope of NFTs subject to AML/CTF regulation be clarified?** NFTs have many use cases and the scope of NFTs subject to AML/CTF regulation should consider each of these. The purpose of an NFT can change over time. For example, an NFT can be minted as a collectible and later be used as a form of investment. The purpose and any changes in the purpose of the NFT are not always known at the outset. Further, as another example, Uniswap V3 liquidity positions are represented as NFTs. These NFTs are neither a means of payment, nor an investment instrument, nor are they collectibles. It is unclear from the proposed framework whether these NFTs would be regulated. With regard to NFTs used as payments, in gaming, it is common for in-game items to be traded for another in-game item. This applies to both Web2 games and Web3 games. Further, often Web3 games will have 'crafting', 'burning' or 'sacrificing' mechanics where one NFT is taken out of circulation in return for another NFT or an entertainment function. These examples are not payment mechanics and should not be captured under AML/CTF obligations. With regard to NFTs used as collectibles as opposed to investments; both collectibles and investments may have a market value. A consumer may collect a gaming-related NFT in order to consume it in-game or for its in-game utility. However, if the same NFT also has a secondary market value or happens to gain value, it is unclear if it would become an investment? We suggest that there would need to be a test for whether an NFT is to be considered an investment. <u>Recommendation</u> We suggest that clarity is needed around the circumstances when an NFT would be viewed as a payment, whilst balancing policy objectives

Topic	Response
	and risks. Further, clarity is also needed regarding when an NFT is to be considered an investment. We recommend in-depth analysis of the use cases to set the definitions, along with worked examples.
Clarification regarding definition of 'custody'	**d. Is the proposed language around custody of digital assets or private keys clear?** We are of the opinion that the language and examples provided are helpful in providing clarity around custody of private keys and digital assets. However, providers within the industry will commonly use software that utilises MPC (multi-party computation) technology in order to custody customers' private keys and digital assets. This technology is underpinned by the notion of 'sharding' of the private keys of digital assets held within the software, with the private key 'shards' held by multiple different parties. Commonly, the providers of MPC (multi-party computation) technology software will often be one of the holders of a 'shard' of a private key related to a customer's digital asset held within the software. Recommendation We propose that where this arrangement is in place, the provider of the MPC technology should not be subject to AML/CTF regulation despite holding a 'shard' of a private key, on the basis that they are merely a technology provider. Requiring MPC technology providers to be subjected to AML/CTF regulation will place an unnecessary burden on these technology providers and create unnecessary friction in the process. There is also the risk that these technology providers may stop servicing Australian customers for the risk of being captured by AML/CTF regulation.

4.2 Updates to the travel rule

Topic	Response to consultation questions

The sunrise issue	**i. What flexibility should be permitted to address the sunrise issue or where a financial institution or digital asset service provider has doubts about an overseas counterparty's implementation of adequate data security and privacy protections? What risk mitigation measures should be required?** **Risk-based approach** It is important to allow a risk-based approach to the Travel Rule in order to address the sunrise issue or doubts about counterparties. Being one of the last FATF members to implement the Travel Rule, Australia should pay close attention to lessons learned from other members. For example, the FCA allows a risk-based approach where the country of the counterparty can be determined, however this is often not possible for Digital Asset Service Providers (DASPs). Applying a risk-based approach is sensible, however adequate guidance must be provided and applicability to each industry sector must be considered. <u>Recommendation</u> We submit that the Attorney-General's Department provide guidance regarding risk-based measures that could be employed by DASPs, which could include: • Reasonable steps to obtain required information from counterparty • Reasonable steps to confirm there is no sending or receiving exposure to sanctioned or high risk jurisdictions/entities **Protection of Australian customer PII** In Japan and the U.K., if the counterparty is located in a region without Travel Rule enforcement, VASPs are still required to collect and retain information about the counterparty and assess money laundering / terrorist financing risks. The VASPs may proceed with the transaction but have no obligation to transmit Travel Rule information. Allowing the same flexibility for Australian DASPs will help protect Australian

	customers' personally identifiable information (PII) while still collecting the required information where it is possible. Recommendation To protect customer PII, we submit that the Attorney-General's Department removes the obligation to transmit Travel Rule information if the transacting counterparty is located in a region without Travel Rule enforcement. We recommend additional effort is made to determine and strike the appropriate balance between combating financial crime and protecting customer data privacy. **Continued transactions** Globally, the Travel Rule has created much friction and frustration for customers due to the additional questioning and customer declarations required. Particularly where transactions must be halted due to insufficient travel rule information. In the U.K., if a VASP receives a transaction without the required Travel Rule information, the VASP is permitted to make a risk-based determination on whether to make the digital asset available to the beneficiary, taking into account the status of Travel Rule regulations in the jurisdiction where the originator VASP operates. Recommendation Where reasonable steps have been taken, we propose that DASPs should be permitted to make risk-based determinations on whether to proceed with the transaction in question. **Transition period** To minimise impact to transaction flows, DASPs may need to use more than one vendor to ensure Travel Rule interoperability with one another. Interoperability is critical for ensuring the various Travel Rule messaging protocols and their networks exchange PII effectively without compromising safety and security. Due to the significant vendor arrangements, system setup and resource diversions needed

	for the implementation of Travel Rule, a reasonable 'ramp-up' period is needed to meet requirements. Consideration should also be given to the operational and cost implications of implementation. It may be difficult for smaller entities to bear the costs associated with Travel Rule compliance which may result in seeking support or shared solutions within industry. Global exchanges have experienced roll-out timeframes of 24-36 months, because of the need to integrate different software providers across multiple jurisdictions. Recommendation We recommend a minimum transition period of 24 months from the policy effective date.
Travel Rule exemptions	**j. Do you consider that the existing exemptions for the travel rule are appropriately balanced?** **Further guidance needed on subset of information required** In order to comply with the AML/CTF framework, DASPs will need to collect information about both the payer and payee of the funds and implement a risk framework that actively measures the AML/CTF risk of the transaction. In practice, this requires DASPs to agree on how this is done and use a common interface that allows for the timely and secure sharing of sensitive information. The consultation paper states that, in these circumstances, "a subset of information sufficient to trace the transaction through the value transfer chain may be transmitted instead." However, the paper does not indicate what form the subset of information should be. Recommendation We propose that the Attorney-General's Department provide further guidance regarding the subset of information required. **The decentralised economy**

	Whilst software decentralised online wallet providers originally gave clients an independent self-custody solution for individuals, many of these wallets are adopting new technologies and becoming decentralised smart wallets facilitating token swaps, staking and other services that would be traditionally offered by a licensed DASP. Australian AML/CTF regulation should consider an ongoing review of its Digital Asset Service Provider DASP definition to ensure that licensed, centralised and Travel Rule-compliant DASPs are not disadvantaged by decentralised smart wallet companies who are benefitting from Travel Rule exemptions. Recommendation We ask the Attorney-General's Department to ensure that data transmission complies with data protection laws both in Australia and overseas.
Reporting of cross-border transfers	**k. Are there challenges for financial institutions reporting cross-border transfers of digital assets, including stablecoins, on behalf of customers?** **Clarification needed on Travel Rule reporting** Page 12 of the consultation paper states: "The travel rule is a record-keeping and data transmission requirement, not a reporting requirement." Recommendation We ask that the Attorney-General's Department please clarify the reporting requirement referred to in this question.
Transfers to Foreign Exchange and Gambling Services	**i. Should the travel rule apply when transferring value incidental to a foreign exchange or gambling service?** It is likely that a number of these service providers, particularly offshore service providers, or providers who are based in a jurisdiction where the Travel Rule has not been implemented, will not capture or provide information required to be collected under Travel Rule

	obligations. Imposing Travel Rule obligations on transfers to these providers may likely be operationally impractical. Recommendation We propose that the Travel Rule not apply when transferring value incidental to a foreign exchange or gambling service.

4.3 Reforms to IFTI reports

Topic	**Response to consultation questions**
'Trigger' for IFTI reporting	**n. What should be the 'trigger' for reporting IFTIs?** We agree that IFTI reporting should be triggered by the reporting entity sending value, or making the value available to the customer, rather than by the sending or receipt of an instruction. From the DCE perspective, successful transfers of value can be confirmed using transaction hash or transaction ID numbers, which are unique identifiers used to monitor blockchain transactions. Recommendation We submit that the Attorney-General's Department adopt the change to the trigger for IFTI reporting and ask that a taxonomy be developed that can be applied to both traditional financial services as well as digital asset financial services.

Reporting Requirements of IFTI	**o. What information should be required to be reported in a unified IFTI reporting template, covering both IFTI-Es and IFTI-DRAs?** **Gaps in information required to be reported** According to the AUSTRAC website, the information required to be reported includes: Full legal name of sender/payer and receiver/beneficiary, ID type, ID number, customer physical address, transfer instruction details, and preferably IP address or device ID for online customers, which would include 100% of DCE customers. Typically, DCEs do not have access to payer or beneficiary information unless the payer or beneficiary is a customer of the DCE. This also applies to payer or beneficiary ID type, ID number, physical address, IP address and device ID information. Offshore entities are unlikely to cooperate or provide this information where there is no legal or regulatory requirement for them to do so. Thus the information required to be reported appears onerous. For DCEs, the ability to fully comply with IFTI reporting requirements will be dependent on effective Travel Rule implementation. Where the Travel Rule implementation is effective, this may assist in obtaining the required information for non-customers. The current requirements are unclear. Currently, law firms look at AUSTRAC's schema titled "Electronic report file format specification - international funds transfer instruction under a designated remittance arrangement (v 1.2, July 2010)", AUSTRAC's IFTI-DRA paper lodgement form, the Act and the Rules, to piece together what each field title means, including the right category for each party in the transaction chain. Legal advice analysing one single inbound transaction and one single outbound transaction (and associated fields) can easily exceed 30 pages. <u>Recommendation</u> We suggest that the reporting requirement for DASPs be reduced, or allow for voluntary compliance until the travel rule is effective. Reduced information required to be reported would include: Customer full name, customer date of birth, customer address on file

	and details of transfer. Definitions should be consistent across the Act, Rules, Schema and Guidance, with worked examples. **Secure method of reporting needed** Canada's Fintrac has been offline for over 3 months since being targeted for a cyber attack in March, creating a potential intelligence gap and possibly increasing the money laundering or terrorist financing risk for Canada. A secure method for reporting is critical. Unlike banks, DASPs do not use the SWIFT network and there is no SWIFT-equivalent for DASPs for securely sending data between parties. There is currently no functionality provided by AUSTRAC for an equivalent integrated secure reporting. Manual reporting will be labour intensive and poses a significant consumer risk and security risk. DASPs are already a honey pot for cyber attacks, and this further increases vulnerability. Considering the volume and frequency of PII required to be reported, options for more secure methods of reporting will need to be explored. <u>Recommendation</u> We propose that AUSTRAC work with DASPs to provide an integrated secure reporting option for DASPs with a transition period following the implementation of the Travel Rule.
Challenges for DASPs	**p. Are there challenges with digital asset service providers reporting IFTIs to AUSTRAC as proposed?** **The geographic test for DASPs is problematic** The proposed geographic test for IFTIs related to digital asset transfers would be tied to either: (a) the overseas location of a counterparty's permanent establishment or (b) an overseas jurisdiction in which the overseas counterparty is registered or licensed. On point (b) however, it is difficult to know where the transacting entity is located or where it is registered or licensed (if at all). An international DCE will have multiple legal entities and multiple permanent establishments. On-chain analysis tools may tag an omnibus wallet address to an exchange but it does not include the legal entity name nor information about registrations or licences.

	For DCEs, the ability to comply with IFTI reporting requirements will be dependent on effective Travel Rule implementation - assuming the required Travel Rule information will include DCE location of permanent information and/or jurisdiction of DCE registration/licence. Without this information, DCEs may be forced to over-report IFTIs where they are unable to perform the geographic test. Recommendation We propose that reporting requirements for DASPs are reduced, or allow for voluntary compliance until the Travel Rule is effective. The reduced reporting requirement may entail IFTI reporting only where the DCE is able to confirm the transacting counterparty is offshore. **Lack of supporting infrastructure and data sources** Functionality is provided by AUSTRAC for banks to integrate Swift messaging infrastructure with IFTI reporting, which enables secure and automated reporting. However, equivalent functionality is required for DASPs. The information required to be reported and the geographic test assume access to payer/beneficiary and DCE information that is currently not available. If the required information is included as part of Travel Rule requirements, DCEs and DASP compliance with the IFTI reporting requirements may be easier, so long as the transacting counterparty is willing to cooperate. **Critical dependency on Travel Rule and counterparty cooperation** There will be a critical dependency on the effective implementation of Travel Rule in order for DCEs to fully comply with IFTI reporting requirements. Once the Travel Rule is implemented, cooperation from offshore counterparties is needed to obtain the information required to be reported. Offshore entities not subject to Australian rules and regulations may not see value in setting up systems to enable Australian entities to comply with the IFTI reporting requirements. **Self-hosted wallets**

	The IFTI regime will not be appropriate for self-hosted wallets until the Travel Rule is implemented and adequate guidance is provided on how the information collection requirement is to be met. For example, would Enhanced Due Diligence be sufficient? Or is identity verification of the self-hosted wallet owner required? Recommendation We recommend against the application of IFTI reporting requirements for self-hosted wallets until such time Travel Rule is implemented and adequate guidance is provided. **Clear guidance needed** We argue that clearer guidelines from AUSTRAC about which reporting requirement takes precedence is needed. For example, if digital assets are used to facilitate a cross-border transaction, should the payout follow the collection and reporting requirements for DCEs or remittance providers? The information required to be reported regarding a receiving beneficiary for a remittance provider is different to the information required to be reported for a DCE. Recommendation We ask that clear guidance is issued by AUSTRAC about which reporting requirement takes precedence.

Blockchain Australia

5. Recommendations to Paper 5: Broader reforms to simplify, clarify and modernise the regime

Topic	Response
Business group head	**a. Under the outlined proposal, a business group head would ensure that the AML/CTF program applies to all branches and subsidiaries. Responsibility for some obligations (such as certain CDD requirements) could also be delegated to an entity within the group where appropriate. For example, a franchisor could take responsibility for overseeing the implementation of transaction monitoring in line with a group-wide risk assessment. Would this proposal assist in alleviating some of the initial costs for smaller entities?** The digital asset industry in Australia currently consists of mostly of: 1. **Domestic Businesses:** These are primarily standalone entities that are not part of larger business groups and currently operate independently and manage their own AML/CTF compliance obligations. For domestic businesses, the proposed model where AML/CTF obligations can be managed by the business group head could reduce the initial compliance cost of developing new business lines where the AML obligations can be met by the group head. This approach, by removing the need to create a 'designated business group' will reduce administrative burden and may support the expansion of new business lines, fostering innovation and growth within the domestic digital asset market. 2. **Australian Subsidiaries of Foreign Business Groups:** These entities are part of larger international organisations with parent companies located outside of Australia. They

Topic	Response
	must navigate both local and international AML/CTF regulations. For Australian subsidiaries of foreign business groups, having clear and unified AML/CTF obligations globally may support consistency in compliance across all jurisdictions where the parent company operates. This harmonisation of rules could make Australia a more attractive destination for business investment. By aligning local regulations with international standards, Australia can enhance its reputation as a business-friendly and compliant environment for digital assets. Recommendation Blockchain Australia is supportive of this recommendation as it streamlines processes, reduces domestic cost-of-innovation, and lowers the barrier to foreign business investment into Australia.
Simplified due diligence	**e. What circumstances should support consideration of simplified due diligence measures?** We are supportive of increased flexibility in the use of simplified due diligence where justified. This will allow DASPs to determine the appropriate risk-based approach to customers who pose a low ML/TF risk. This approach can be unique to their businesses and could also provide more flexibility in the customer experience design. Recommendation We are supportive of proposed simplified due diligence measures

Topic	Response
AUSTRAC guidance	**f. What guidance should AUSTRAC produce to assist reporting entities to meet the expectations of an outcomes-focused approach to CDD?** We commend AUSTRAC for the maintenance of government to industry dialogue established with the industry through Blockchain Australia since the registration of DCEPs in 2018. This open line of communication, sometimes conducted through annual roundtables, have been helpful for the DCEPs/DASPs in both understanding and implementing the policies to meet their obligations. The provision of clear and concise factsheets or guidance notes (with DCE/DASP examples) showing DASPs how AUSTRAC interprets the new requirements will be useful for the DASPs to understand AUSTRAC's expectations, and will also assist with communicating requirements to stakeholders. For example, internally within the DASP organisation and external service providers. <u>Recommendation</u> Provide clear and concise factsheets or guidance notes with DCE and DASP examples showing DASPs how AUSTRAC interprets the new requirements. Continuation of AUSTRAC-to-industry roundtables annually.
Conclusion of business relationship	**g. When do you think should be considered the conclusion of a 'business relationship'?** The defining of 'business relationship' and 'occasional transaction' is common practice in other jurisdictions and would also be welcome by DASPs in Australia. Particularly as this will provide a clear distinction between the CDD measures for each respectively. Blockchain Australia members considered the following as options for defining the conclusion of a 'business relationship': ● Closure of the account

Topic	Response
	• Open but inactive account over a specified period of time with low balance (e.g. no active transactions for 2 years with $1 balance) • Restricted account over a specified period of time with abandoned funds (e.g. account restricted for 9 months at law enforcement's request with $500 balance) Accounts where a 'keep open' notice has been received should also be exempt from EDD and OCDD requirements. <u>Recommendation</u> Recommend adoption of definitions for 'business relationship' and 'occasional transaction'. Recommend provision of guidance around how lost or abandoned funds should be treated.
Tipping off offence	**i. Are there situations where SMR or section 49 related information may need to be disclosed for legitimate purposes but would still be prevented by the proposed framing of the offence?** Blockchain Australia members are supportive of the proposal to reframe the tipping off offence. On many occasions, DASPs have attempted to share information between one another with the aim of preventing scams. However these attempts were met with limited success due to concerns over tipping off and privacy. The Fraud Reporting Exchange (FRX) portal has the potential to achieve far greater results if private-to-private information sharing can be facilitated. Clarity and guidance is also needed on which agencies information can be shared with, and in which scenarios. For example, a DASP offboards a customer for ML/TF reasons and the customer lodges a complaint to AFCA about the unwanted account termination. In handling the complaint, the AFCA case manager asks the DASP

Topic	Response
	about the reason for account termination, and also requests supporting documentation. What information should and should not be shared with AFCA? <u>Recommendation</u> Recommend adoption of the reframed tipping off offence. Recommend provision of explicit guidance around when information can be shared with specific agencies, and specifically what information can be shared. For example, when can information be shared with AFCA? Recommend also making further amendments to facilitate private-to-private information sharing subject to appropriate protections being in place.

6. Concluding Remarks

The Blockchain Australia membership base consists of 130+ leading cryptocurrency and Blockchain centric businesses and 115+ individuals across multiple verticals including:

- Accounting and Taxation
- Artificial Intelligence
- Banking
- Cyber Security
- Development
- Building & Construction
- Digital ID
- Energy and Resources
- Art & Entertainment
- Gaming
- Health and Wellbeing
- Insurance
- Investment
- Legal
- Recruitment
- Real Estate
- Risk and Compliance
- Supply Chain
- Venture Capital
- Custody

We give thanks to the Attorney General's Department for taking the time to consider our submission and welcome any opportunity for further dialogue.

Rebranding

We wish to advise that Blockchain Australia is rebranding to the Digital Economy Council of Australia (DECA) over the coming weeks. We remain committed to advocating for clear and effective regulatory frameworks that support innovation and compliance within the digital economy.